Guia de Administração

SUSE Linux Enterprise Desktop 12

Guia de Administração

SUSE Linux Enterprise Desktop 12

Abrange tarefas de administração do sistema, como manutenção, monitoramento e personalização de um sistema instalado inicialmente.

data de publicação: 15 de outubro de 2014

SUSE Linux Products GmbH
Maxfeldstr. 5
90409 Nürnberg
GERMANY
https://www.suse.com/documentation

Copyright © 2006–2014 SUSE LLC e colaboradores. Todos os direitos reservados.

Permissão concedida para copiar, distribuir e/ou modificar este documento sob os termos da Licença GNU de Documentação Livre, Versão 1.2 ou (por sua opção) versão 1.3; com a Seção Invariante sendo estas informações de copyright e a licença. Uma cópia da versão 1.2 da licença está incluída na seção intitulada “GNU Free Documentation License” (Licença GNU de Documentação Livre).

Para ver as marcas registradas da Novell e SUSE, consulte a lista de Marcas Registradas e Marcas de Serviço da Novell http://www.novell.com/company/legal/trademarks/tmlist.html. Todas as outras marcas registradas de terceiros pertencem aos seus respectivos proprietários. Um símbolo de marca registrada (®, ™ etc.) indica uma marca registrada da Novell ou SUSE; um asterisco (*) indica uma marca registrada de terceiros.

Todas as informações deste manual foram compiladas com a maior atenção possível aos detalhes. Entretanto, isso não garante uma precisão absoluta. A SUSE LLC, suas afiliadas, os autores ou tradutores não serão responsáveis por possíveis erros nem pelas consequências resultantes de tais erros.

Sumário

Sobre este guia xvi

I SUPORTE E TAREFAS COMUNS 1

1 Atualização Online do YaST 2

1.1 Caixa de diálogo Atualização Online 3

1.2 Instalando patches 4

1.3 Atualização online automática 5

2 Reunindo informações do sistema para suporte 7

2.1 Exibindo informações atuais do sistema 7

2.2 Coletando informações do sistema com o supportconfig 8

Criando um número de solicitação de serviço 8 • Destinos de upload 9 • Criando um armazenamento supportconfig com o YaST 9 • Criando um armazenamento supportconfig da linha de comando 11 • Opções comuns do supportconfig 12

2.3 Submetendo informações ao suporte técnico global 13

2.4 Analisando informações do sistema 15

Ferramenta de linha de comando SCA 16 • Aplicação SCA 17 • Desenvolvendo padrões de análise personalizados 30

2.5 Suporte aos módulos do Kernel 30

Informações técnicas 31 • Trabalhando com módulos não suportados 31

2.6 Para obter mais informações 32

3 YaST em modo de texto 34

3.1 Navegação em módulos 35

3.2 Restrição de combinações de tecla 36

3.3 Opções de linha de comando do YaST 37

Iniciando os módulos individuais 37 • Instalando pacotes a partir da linha de comando 38 • Parâmetros de linha de comando dos módulos do YaST 38

4 Recuperação de sistema e gerenciamento de instantâneos com o Snapper 39

4.1 Configuração padrão 40

Personalizando a configuração 42

4.2 Usando o Snapper para desfazer mudanças 45

Desfazendo mudanças do YaST e Zypper 47 • Usando o Snapper para restaurar arquivos 52

4.3 Rollback do sistema por inicialização de instantâneos 54

Limitações 56

4.4 Criando e modificando as configurações do Snapper 57

Gerenciando configurações existentes 58

4.5 Criando e gerenciando instantâneos manualmente 63

Metadados de instantâneos 63 • Criando instantâneos 65 • Modificando os metadados do instantâneo 66 • Apagando instantâneos 67

4.6 Perguntas mais frequentes 68

5 Acesso remoto com VNC 69

5.1 Sessões VNC únicas 69

Iniciando uma sessão VNC única 70 • Configurando sessões VNC únicas 70

5.2 Sessões VNC persistentes 71

Conectando-se a uma sessão VNC persistente 73 • Configurando sessões VNC persistentes 74

6 Configuração do GNOME para administradores 75

6.1 Iniciando aplicativos automaticamente 75

6.2 Montando automaticamente e gerenciando dispositivos de mídia 75

6.3 Mudando os aplicativos preferenciais 76

6.4 Adicionando modelos de documentos 76

6.5 Para obter mais informações 76

7 Gerenciando software com ferramentas de linha de comando 77

7.1 Usando o zypper 77

Uso geral 77 • Instalando e removendo software com o zypper 79 • Atualizando software com o zypper 82 • Gerenciando repositórios com o zypper 85 • Consultando repositórios e pacotes com o zypper 87 • Configurando o Zypper 89 • Solucionando problemas 89 • Recurso de rollback do Zypper no sistema de arquivos Btrfs 89 • Para obter mais informações 90

7.2 RPM — o gerenciador de pacotes 90

Verificando a autenticidade do pacote 91 • Gerenciando pacotes: instalar, atualizar e desinstalar 91 • Pacotes RPM Delta 93 • Consultas de RPM 94 • Instalando e compilando pacotes de fonte 97 • Compilando pacotes RPM com build 99 • Ferramentas para arquivos RPM e banco de dados RPM 99

8 Bash e scripts Bash 101

8.1 O que é “o shell”? 101

Conhecendo os arquivos de configuração do Bash 101 • Estrutura de diretórios 102

8.2 Gravando scripts shell 107

8.3 Redirecionando eventos de comando 108

8.4 Usando álias 109

8.5 Usando variáveis no Bash 109

Usando variáveis de argumento 111 • Usando substituição de variável 111

8.6 Agrupando e combinando comandos 112

8.7 Trabalhando com construções de fluxo comuns 113

Comando de controle if 114 • Criando loops com o comando for 114

8.8 Para obter mais informações 115

II SISTEMA 116

9 Aplicativos de 32 bits e 64 bits em um ambiente de sistema de 64 bits 117

9.1 Suporte ao tempo de execução 117

9.2 Desenvolvimento de software 118

9.3 Compilação de software em plataformas biarch 118

9.4 Especificações do kernel 120

10 Inicializando um sistema Linux 121

10.1 Processo de boot do Linux 121

10.2 `initramfs` 123

10.3 init no `initramfs` 124

11 O daemon `systemd` 126

11.1 O conceito do systemd 126

O que é systemd 126 • Arquivo unit 127

11.2 Uso básico 128

Gerenciando serviços em um sistema em execução 128 • Habilitando/Desabilitando serviços permanentemente 130

11.3 Inicialização do sistema e gerenciamento de destino 132

Destinos X níveis de execução 132 • Depurando a inicialização do sistema 136 • Compatibilidade com o System V 140

11.4 Gerenciando serviços com o YaST 141

11.5 Personalização do `systemd` 142
Personalizando arquivos de serviço 142 • Criando arquivos "dropin" 143 • Criando destinos personalizados 143

11.6 Uso avançado 144
Registro do Sistema 144 • Instantâneos 144 • Carregamento de módulos Kernel 145 • Grupos de controle (cgroups) do Kernel 145 • Terminando os serviços (enviando sinais) 147 • Depurando serviços 148

11.7 Mais informações 149

12 `journalctl`: consultar o diário do `systemd` 150

12.1 Tornando o diário persistente 150

12.2 Switches úteis do **`journalctl`** 151

12.3 Filtrando a saída do diário 152
Filtrando com base em um número de boot 152 • Filtrando com base no intervalo de tempo 153 • Filtrando com base nos campos 154

12.4 Investigando erros do `systemd` 155

12.5 Configuração do journald 156
Mudando o limite de tamanho do diário 157 • Encaminhando o diário para `/dev/ttyX` 157 • Encaminhando o diário para o recurso do syslog 157

13 O carregador de boot GRUB 2 158

13.1 Principais diferenças entre o GRUB Legacy e o GRUB 2 158

13.2 Estrutura do arquivo de configuração 158
O arquivo `/boot/grub2/grub.cfg` 160 • O arquivo `/etc/default/grub` 160 • Scripts em `/etc/grub.d` 163 • Mapeamento entre unidades BIOS e dispositivos Linux 164 • Editando as entradas de menu durante o procedimento de boot 165 • Configurando uma senha de boot 167

13.3 Configurando o carregador de boot com o YaST 168
Mudando o tipo de carregador de boot 169 • Modificando a localização do carregador de boot 170 • Ajustando a ordem dos discos 170 • Configurando as opções avançadas 171

13.4 Diferenças no uso de terminais no System z 174
Limitações 174 • Combinações de tecla 175

13.5 Comandos úteis do GRUB 2 177

13.6 Mais informações 178

14 UEFI (Unified Extensible Firmware Interface) 179

14.1 Boot seguro 179
Implementação no SUSE Linux Enterprise 180 • MOK (Chave do Proprietário da Máquina) 183 • Inicializando um kernel personalizado 183 • Recursos e limitações 186

14.2 Para obter mais informações 187

15 Recursos especiais do sistema 188

15.1 Informações sobre pacotes de software especiais 188
O pacote `bash` e `/etc/profile` 188 • O pacote cron 189 • Parando mensagens de status do Cron 190 • Arquivos de registro: pacote logrotate 191 • O comando locate 192 • O comando ulimit 192 • O comando free 193 • Páginas de manual e de informações 194 • Selecionando páginas de manual usando o comando **`man`** 194 • Configurações para GNU Emacs 195

15.2 Consoles virtuais 196

15.3 Mapeamento de teclado 196

15.4 Configurações de idioma e específicas de país 197
Alguns exemplos 198 • Configurações locais em `~/.i18n` 199 • Configurações de suporte de idioma 200 • Para obter mais informações 201

16 Operação da impressora 202

16.1 O workflow do CUPS 203

16.2 Métodos e protocolos de conexão de impressoras 204

16.3 Instalando o software 204

16.4 Impressoras de rede 205

16.5 Configurando o CUPS com ferramentas da linha de comando 206

16.6 Imprimindo pela linha de comando 208

16.7 Recursos especiais no SUSE Linux Enterprise Desktop 208
CUPS e firewall 208 • Procurando impressoras de rede 209 • Arquivos PPD em pacotes diferentes 210

16.8 Solução de problemas 210
Impressoras sem suporte de linguagem de impressora padrão 210 • Nenhum arquivo PPD adequado disponível para impressora PostScript 211 • Conexões da impressora de rede 212 • Defeitos na impressão sem mensagem de erro 215 • Filas desabilitadas 215 • Navegação do CUPS: apagando serviços de impressão 215 • Serviços de impressão com defeito e erros de transferência de dados 216 • Depurando o CUPS 216 • Para obter mais informações 217

17 Gerenciamento dinâmico de dispositivos do Kernel com udev 218

17.1 O diretório /dev 218

17.2 uevents e udev do Kernel 219

17.3 Drivers, módulos de kernel e dispositivos 219

17.4 Inicialização e configuração do dispositivo inicial 220

17.5 Monitorando o daemon udev em execução 220

17.6 Influenciando o gerenciamento de eventos de dispositivo do Kernel com as regras do udev 222
Usando operadores nas regras do udev 224 • Usando substituições nas regras do udev 225 • Usando as chaves de correspondência do udev 226 • Usando as chaves de atribuição do udev 227

17.7 Nomeação de dispositivo persistente 229

17.8 Arquivos usados pelo udev 230

17.9 Para obter mais informações 231

18 O sistema X Window 232

18.1 Instalando e configurando fontes 232

Mostrando as fontes instaladas 233 • Vendo fontes 234 • Consultando fontes 234 • Instalando fontes 235 • Configurando a aparência das fontes 236

18.2 Para obter mais informações 246

19 Acessando sistemas de arquivos com o FUSE 247

19.1 Configurando o FUSE 247

19.2 Plug-ins disponíveis do FUSE 247

19.3 Para obter mais informações 248

III SERVIÇOS 249

20 Rede básica 250

20.1 Roteamento e endereços IP 253

Endereços IP 254 • Máscaras de rede e roteamento 254

20.2 IPv6 — A Internet da próxima geração 256

Vantagens 257 • Estrutura e tipos de endereços 259 • Coexistência de IPv4 e IPv6 263 • Configurando o IPv6 264 • Para obter mais informações 265

20.3 Resolução de nomes 265

20.4 Configurando uma conexão de rede com o YaST 267

Configurando a placa de rede com o YaST 267

20.5 NetworkManager 279

NetworkManager e **`wicked`** 279 • Funcionalidade do NetworkManager e arquivos de configuração 280 • Controlando e bloqueando recursos do NetworkManager 281

20.6 Configurando uma conexão de rede manualmente 281
Configuração de rede com o **wicked** 281 • Arquivos de configuração 289 • Testando a configuração 299 • Arquivos unit e scripts de inicialização 302

20.7 Configurando dispositivos de ligação 303
Hotplug de escravos associados 306

21 Sincronização de horário com NTP 308

21.1 Configurando um cliente NTP com YaST 308
Configuração Básica 308 • Mudando a configuração básica 309

21.2 Configurando manualmente o NTP na rede 312

21.3 Sincronização de horário dinâmica em tempo de execução 312

21.4 Configurando um relógio de referência local 313

22 Usando o NetworkManager 315

22.1 Casos de uso para o NetworkManager 315

22.2 Habilitando ou desabilitando o NetworkManager 315

22.3 Configurando conexões de rede 316
Gerenciando conexões de rede com fio 318 • Gerenciando conexões de rede wireless 318 • Configurando a placa Wi-Fi/Bluetooth como ponto de acesso 319 • NetworkManager e VPN 319

22.4 NetworkManager e segurança 320
Conexões de usuário e sistema 321 • Armazenando senhas e credenciais 321

22.5 Perguntas mais frequentes 321

22.6 Solução de problemas 323

22.7 Para obter mais informações 324

23 Samba 325

23.1 Terminologia 325

23.2 Instalando um servidor Samba 326

23.3 Configurando um servidor Samba 327

23.4 Configurando clientes 327

Configurando um cliente Samba com o YaST 327

23.5 Samba como servidor de login 327

23.6 Tópicos avançados 328

Compactação de arquivos transparente no Btrfs 329 • Instantâneos 330

23.7 Para obter mais informações 339

24 Compartilhando sistemas de arquivos com o NFS 340

24.1 Terminologia 340

24.2 Instalando o servidor NFS 341

24.3 Configurando clientes 341

Importando sistemas de arquivos com o YaST 341 • Importando sistemas de arquivos manualmente 342 • NFS paralelo (pNFS) 344

24.4 Para obter mais informações 345

25 Montagem sob demanda com o Autofs 346

25.1 Instalação 346

25.2 Configuração 346

O arquivo de mapa master 346 • Arquivos de mapa 349

25.3 Operação e depuração 350

Controlando o serviço `autofs` 350 • Depurando problemas do automounter 350

25.4 Montando automaticamente um compartilhamento NFS 351

25.5 Tópicos avançados 353
Ponto de montagem /net 353 • Usando curingas para montar subdiretórios automaticamente 353 • Montando automaticamente o sistema de arquivos CIFS 354

26 Sincronização de arquivos 355

26.1 Software de sincronização de dados disponível 355
CVS 356 • rsync 356

26.2 Determinando fatores para selecionar um programa 356
Cliente/Servidor X não hierarquia 356 • Portabilidade 357 • Interativo versus automático 357 • Conflitos: incidência e solução 357 • Selecionando e adicionando arquivos 357 • Histórico 358 • Volume de dados e requisitos do disco rígido 358 • GUI 358 • Facilidade de uso 358 • Segurança contra ataques 359 • Proteção contra perda de dados 359

26.3 Introdução ao CVS 360
Configurando um servidor CVS 360 • Usando o CVS 361

26.4 Introdução ao rsync 362
Configuração e operação 363

26.5 Para obter mais informações 364

IV COMPUTADORES MÓVEIS 366

27 Computação móvel com o Linux 367

27.1 Laptops 367
Conservação de energia 367 • Integração em ambientes operacionais variáveis 368 • Opções de software 370 • Segurança de dados 376

27.2 Hardware móvel 377

27.3 Telefones celulares e PDAs 378

27.4 Para obter mais informações 378

28 Gerenciamento de energia 379

28.1 Funções de economia de energia 379

28.2 Advanced Configuration and Power Interface (ACPI) 380
Controlando o desempenho da CPU 381 • Solução de problemas 381
28.3 Descanso do disco rígido 383
28.4 Solução de problemas 385
A frequência da CPU não funciona 385
28.5 Para obter mais informações 385

V SOLUÇÃO DE PROBLEMAS 386

29 Ajuda e documentação 387
29.1 Diretório da documentação 387
Manuais do SUSE 388 • Documentação do pacote 388
29.2 Páginas de manual 389
29.3 Páginas de informações 391
29.4 Recursos Online 391

30 Problemas comuns e suas soluções 393
30.1 Localizando e reunindo informações 393
30.2 Problemas de instalação 396
Verificação de mídia 396 • Nenhuma unidade de DVD inicializável disponível 397 • Falha na inicialização da mídia de instalação 398 • Falha na inicialização 400 • Falha na inicialização do instalador gráfico 402 • Apenas a tela de boot simples é aberta 403
30.3 Problemas de boot 404
Falha ao carregar o carregador de boot GRUB 2 404 • Não é exibido nenhum prompt nem tela de login 405 • Não há login gráfico 405 • Não é possível montar a partição Btrfs raiz 406
30.4 Problemas de login 406
Falha nas combinações de nome de usuário e senha válidas 407 • Nome de usuário e senha não aceitos 408 • Falha de login na partição pessoal

criptografada 410 • Login bem-sucedido, mas há falha na área de trabalho do GNOME 411

30.5 Problemas de rede 412

Problemas no NetworkManager 416

30.6 Problemas de dados 417

Gerenciando imagens de partição 417 • Usando o sistema de recuperação 418

A Atualizações da Documentação 426

A.1 Outubro de 2014 (Versão Inicial do SUSE Linux Enterprise Desktop 12) 426

B Rede de exemplo 431

C GNU Licenses 432

C.1 GNU Free Documentation License 432

Sobre este guia

Este guia é destinado a administradores profissionais de rede e sistema durante a operação do SUSE® Linux Enterprise. Sendo assim, ele se compromete exclusivamente em garantir que o SUSE Linux Enterprise seja configurado apropriadamente e que os serviços requisitados na rede estejam disponíveis para permitir que ele funcione perfeitamente logo após a instalação inicial. Este guia não abrange o processo que garante que o SUSE Linux Enterprise ofereça compatibilidade apropriada ao software aplicativo da sua empresa ou que sua funcionalidade principal atenda a tais requisitos. Ele assume que foi feita uma auditoria completa dos requisitos e que foi solicitada a instalação ou uma instalação de teste, visando tal auditoria.

Este guia contém o seguinte:

Suporte e tarefas comuns

O SUSE Linux Enterprise oferece uma ampla variedade de ferramentas para personalizar diversos aspectos do sistema. Esta parte apresenta algumas delas.

Sistema

Aprenda mais sobre o sistema operacional subjacente estudando esta parte. O SUSE Linux Enterprise suporta várias arquiteturas de hardware e, com isso, você pode adaptar seus próprios aplicativos para serem executados no SUSE Linux Enterprise. As informações do carregador de boot e do procedimento de boot ajudam você a compreender como o sistema Linux funciona e como os seus próprios aplicativos e scripts personalizados podem se fundir a ele.

Serviços

O SUSE Linux Enterprise foi projetado para ser um sistema operacional de rede. O SUSE® Linux Enterprise Desktop inclui suporte de cliente para muitos serviços de rede. Ele se integra bem em ambientes heterogêneos, inclusive clientes e servidores MS Windows.

Computadores móveis

Os laptops, e a comunicação entre dispositivos móveis como PDAs ou telefones celulares, e o SUSE Linux Enterprise requerem atenção especial. Cuide da conservação da energia e da integração de diferentes dispositivos a um ambiente de rede que está sofrendo mudanças. Tenha contato também com tecnologias de segundo plano que fornecem a funcionalidade necessária.

Solução de problemas

Apresenta uma visão geral de onde encontrar ajuda e documentação adicional caso você precise de mais informações ou queira realizar tarefas específicas no sistema. Encontre também uma compilação dos problemas e erros mais frequentes e saiba como resolvê-los sozinho.

Muitos capítulos neste manual contêm links para recursos adicionais de documentação. Isso inclui documentação adicional disponível no sistema assim como documentação disponível na Internet.

Para obter uma visão geral da documentação disponível para o seu produto e das atualizações de documentação mais recentes, consulte http://www.suse.com/doc.

1 Documentação disponível

Fornecemos versões em HTML e PDF de nossos livros em idiomas diferentes. Os seguintes manuais deste produto estão disponíveis para usuários e administradores:

***Artigo* "Inicialização Rápida da Instalação"**

Lista os requisitos do sistema e o orienta passo a passo durante a instalação do SUSE Linux Enterprise Desktop de um DVD ou de uma imagem ISO.

***Book* "Deployment Guide"**

Mostra como instalar sistemas únicos ou vários sistemas e como explorar os recursos inerentes do produto para uma infraestrutura de implantação. Escolha uma das várias abordagens que variam desde uma instalação local ou um servidor de instalação de rede até uma implantação em massa usando uma técnica de instalação remota controlada, automatizada e altamente personalizada.

Guia de Administração

Abrange tarefas de administração do sistema, como manutenção, monitoramento e personalização de um sistema instalado inicialmente.

***Book* "Security Guide"**

Introduz conceitos básicos de segurança do sistema, incluindo aspectos de segurança locais e de rede. Mostra como usar o software de segurança inerente ao produto, como o AppArmor ou o sistema de auditoria que coleta informações sobre todos os eventos relacionados à segurança de forma confiável.

Book "System Analysis and Tuning Guide"

Um guia do administrador para detecção de problema, resolução e otimização. Saiba como inspecionar e otimizar seu sistema através de ferramentas de monitoramento e como gerenciar recursos com eficiência. Também contém uma visão geral dos problemas comuns e soluções e da ajuda adicional e recursos de documentação.

Book "Guia do Usuário do GNOME"

Apresenta a área de trabalho do GNOME do SUSE Linux Enterprise Desktop. Fornece orientações a você durante o uso e a configuração da área de trabalho, além de ajudá-lo a executar tarefas principais. Este manual é destinado principalmente a usuários finais que desejam usar de forma eficiente o GNOME como sua área de trabalho padrão.

Encontre as versões HTML de grande parte dos manuais dos produtos no sistema instalado em `/usr/share/doc/manual` ou nos centros de Ajuda do seu desktop. Obtenha as atualizações mais atuais da documentação em http://www.suse.com/doc de onde você poderá fazer download das versões HTML ou PDF dos manuais referentes ao seu produto.

2 Comentários

Vários canais de comentário estão disponíveis:

Solicitações de bugs e aperfeiçoamentos

Para ver as opções de serviços e suporte disponíveis ao seu produto, consulte http://www.suse.com/support/.

Para relatar bugs de um componente de produto, vá para http://www.suse.com/mysupport, efetue login e selecione *Submit New SR* (Submeter Nova SR).

Comentários do usuário

Nós queremos saber a sua opinião e receber sugestões sobre este manual e outras documentações incluídas neste produto. Utilize o recurso Comentários na parte inferior de cada página da documentação online ou vá para http://www.suse.com/doc/feedback.html e digite lá os seus comentários.

E-mail

Para fazer comentários sobre a documentação deste produto, você também pode enviar um e-mail para `doc-team@suse.de`. Inclua o título do documento, a versão do produto e a data de publicação da documentação. Para relatar erros ou fazer sugestões de melhorias, descreva resumidamente o problema e informe o respectivo número de seção e página (ou URL).

3 Convenções da documentação

As seguintes convenções tipográficas são usadas neste manual:

- `/etc/passwd`: nomes de diretório e arquivo
- *`marcador`*: substitua *`marcador`* pelo valor real
- `PATH`: a variável de ambiente PATH
- **`ls`**, `--help`: comandos, opções e parâmetros
- `user`: usuários ou grupos
- `Alt`, `Alt`–`F1`: uma tecla ou uma combinação de teclas a serem pressionadas; as teclas são mostradas em letras maiúsculas como aparecem no teclado
- *Arquivo*, *Arquivo* › *Gravar Como*: itens de menu, botões
- *Pinguins Dançarinos* (Capítulo *Pinguins*, ↑Outro Manual): É uma referência a um capítulo de outro manual.

I Suporte e tarefas comuns

1 Atualização Online do YaST 2

2 Reunindo informações do sistema para suporte 7

3 YaST em modo de texto 34

4 Recuperação de sistema e gerenciamento de instantâneos com o Snapper 39

5 Acesso remoto com VNC 69

6 Configuração do GNOME para administradores 75

7 Gerenciando software com ferramentas de linha de comando 77

8 Bash e scripts Bash 101

1 Atualização Online do YaST

O SUSE oferece um fluxo contínuo de atualizações de segurança de software para o seu produto. Por padrão, o applet de atualização é usado para manter o sistema atualizado. Consulte a *Book "*Deployment Guide*" 6 "Installing or Removing Software"6.4 "Keeping the System Up-to-date"* para obter mais informações sobre o applet de atualização. Este capítulo aborda a ferramenta alternativa para atualizar pacotes de software: Atualização Online do YaST.

Os patches atuais para o SUSE® Linux Enterprise Desktop estão disponíveis em um repositório de software de atualização. Se você registrou seu produto durante a instalação, já há um repositório de atualização configurado. Se você não registrou o SUSE Linux Enterprise Desktop, poderá fazer isso iniciando a *Configuração do SUSE Customer Center* no YaST. Alternativamente, você pode adicionar manualmente um repositório de atualização de uma fonte confiável. Para adicionar ou remover repositórios, inicie o Gerenciador de Repositórios em *Software* › *Repositórios de Software* no YaST. Saiba mais sobre o Gerenciador de Repositórios na *Book "*Deployment Guide*" 6 "Installing or Removing Software"6.3 "Managing Software Repositories and Services"*.

Nota: erro ao acessar o catálogo de atualização

Se você não conseguir acessar o catálogo de atualização, pode ser que a inscrição tenha expirado. Normalmente, o SUSE Linux Enterprise Desktop vem com uma inscrição de um ou três anos, período em que você terá acesso ao catálogo de atualização. O acesso será negado quando a inscrição terminar.

No caso de negação de acesso ao catálogo de atualização, você verá uma mensagem de aviso com uma recomendação para visitar o SUSE Customer Center e verificar sua inscrição. O SUSE Customer Center está disponível em https://scc.suse.com/.

O SUSE oferece atualizações com diferentes níveis de relevância:

Atualizações de Segurança

Corrigem riscos graves à segurança e sempre devem ser instaladas.

Atualizações Recomendadas

Corrigem problemas que podem comprometer o computador.

Atualizações Opcionais

Corrigem problemas não relacionados à segurança ou aplicam melhorias.

1.1 Caixa de diálogo Atualização Online

Para abrir a caixa de diálogo *Atualização Online* do YaST, inicie o YaST e selecione *Software* › *Atualização Online*. Se preferir, inicie-o usando a linha de comando **`yast2 online_update`**.

A janela *Atualização Online* é composta por quatro seções.

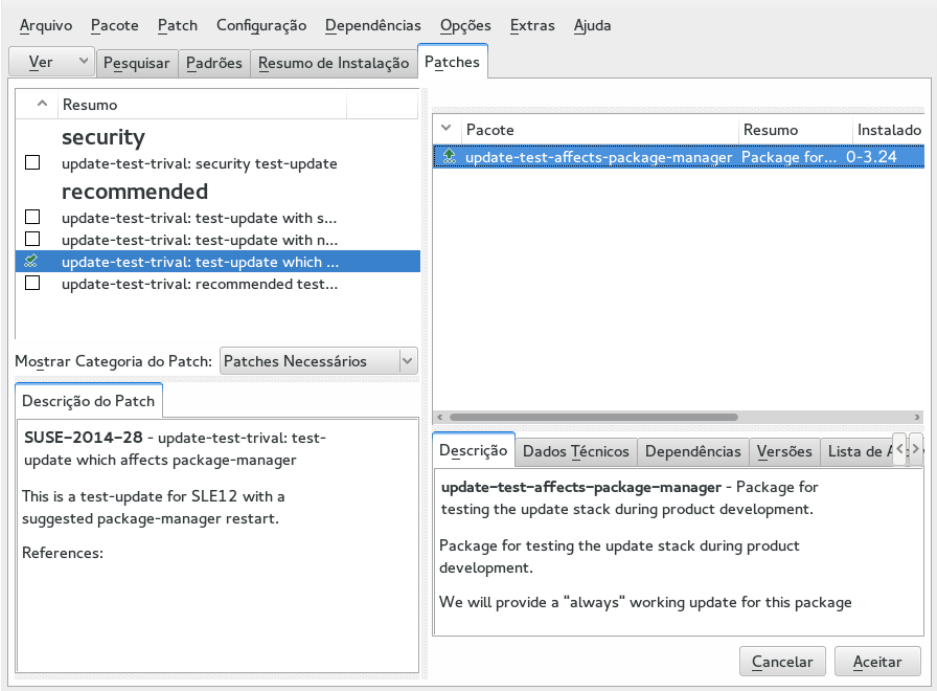

Arquivo Pacote Patch Configuração Dependências Opções Extras Ajuda
Ver Pesquisar Padrões Resumo de Instalação Patches
Resumo
security
update-test-trival: security test-update
recommended
update-test-trival: test-update with s...
update-test-trival: test-update with n...
update-test-trival: test-update which ...
update-test-trival: recommended test...
Mostrar Categoria do Patch: Patches Necessários
Descrição do Patch
SUSE-2014-28 - update-test-trival: test-update which affects package-manager
This is a test-update for SLE12 with a suggested package-manager restart.
References:
Pacote Resumo Instalado
update-test-affects-package-manager Package for... 0-3.24
Descrição Dados Técnicos Dependências Versões Lista de
update-test-affects-package-manager - Package for testing the update stack during product development.
Package for testing the update stack during product development.
We will provide a "always" working update for this package
Cancelar Aceitar

FIGURA 1.1 ATUALIZAÇÃO ONLINE DO YAST

A seção *Resumo* à esquerda lista os patches disponíveis para o SUSE Linux Enterprise Desktop. Os patches são classificados por relevância de segurança: `segurança`, `recomendado` e `opcional`. É possível mudar a tela da seção *Resumo* selecionando uma das seguintes opções em *Mostrar Categoria do Patch*:

***Patches Necessários* (tela padrão)**

Patches não instalados que se aplicam aos pacotes instalados no seu sistema.

Patches Não Necessários

Os patches que se aplicam a pacotes não instalados no seu sistema, ou patches com requisitos que já foram atendidos (porque os pacotes relevantes já foram atualizados de outra fonte).

Todos os Patches

Todos os patches disponíveis para o SUSE Linux Enterprise Desktop.

Cada entrada da lista na seção *Resumo* consiste em um símbolo e no nome do patch. Para obter uma visão geral dos símbolos possíveis e seu significado, pressione Shift–F1. As ações exigidas pelos patches de `Segurança` e `Recomendados` são predefinidas automaticamente. Essas ações são *Instalar automaticamente*, *Atualizar automaticamente* e *Apagar automaticamente*.

Se você instalar um pacote atualizado de um repositório que não seja o repositório de atualização, os requisitos de um patch para esse pacote poderão ser atendidos com essa instalação. Nesse caso, uma marca de seleção é exibida na frente do resumo do patch. O patch ficará visível na lista até você marcá-lo para instalação. Isso na verdade não instalará o patch (porque o pacote já está atualizado), mas marcará o patch como instalado.

Selecione uma entrada na seção *Resumo* para ver uma breve *Descrição do Patch* no canto inferior esquerdo da caixa de diálogo. A seção superior direita lista os pacotes incluídos no patch selecionado (um patch pode incluir vários pacotes). Clique em uma entrada na seção superior direita para ver os detalhes sobre o respectivo pacote que faz parte do patch.

1.2 Instalando patches

A caixa de diálogo Atualização Online do YaST permite instalar todos os patches disponíveis de uma vez ou selecionar manualmente os patches que deseja aplicar ao sistema. É possível também reverter os patches que foram aplicados ao sistema.

Por padrão, todos os novos patches (exceto os `opcionais`) disponíveis para o sistema já estão marcados para instalação. Eles serão aplicados automaticamente depois que você clicar em *Aceitar* ou *Aplicar*. Se um ou vários patches exigirem reinicialização do sistema, você será notificado sobre isso antes do início da instalação do patch. Você escolhe entre continuar a instalação dos patches selecionados, ignorar a instalação de todos os patches que precisam de reinicialização e instalar o restante ou voltar para a seleção manual de patch.

PROCEDIMENTO 1.1 APLICANDO PATCHES COM A ATUALIZAÇÃO ONLINE DO YAST

1. Inicie o YaST e selecione *Software* › *Atualização Online*.
2. Para aplicar automaticamente todos os novos patches (exceto os `opcionais`) disponíveis para o sistema, clique em *Aplicar* ou *Aceitar* para iniciar a instalação dos patches pré-selecionados.
3. Modifique primeiro a seleção dos patches que deseja aplicar:

a. Use os respectivos filtros e telas fornecidos pela interface. Para obter informações detalhadas, consulte a *Seção 1.1, "Caixa de diálogo Atualização Online"*.

b. Selecione ou anule a seleção dos patches de acordo com as suas necessidades e com a sua vontade, clicando o botão direito do mouse no patch e escolhendo a respectiva ação no menu de contexto.

> **Importante: Sempre aplicar as atualizações de segurança**
>
> Não anule a seleção de nenhum patch relacionado à `segurança` se não tiver um bom motivo para isso. Eles corrigem riscos graves à segurança e impedem que o sistema seja explorado.

c. A maioria dos patches inclui atualizações para diversos pacotes. Para mudar as ações de pacotes únicos, clique o botão direito do mouse em um pacote na tela de pacotes e escolha uma ação.

d. Para confirmar sua seleção e aplicar os patches selecionados, clique em *Aplicar* ou *Aceitar*.

4. Após o término da instalação, clique em *Concluir* para sair da *Atualização Online* do YaST. Seu sistema está atualizado.

1.3 Atualização online automática

O YaST também permite configurar uma atualização automática com programação diária, semanal ou mensal. Para usar o respectivo módulo, você precisa instalar primeiro o pacote `yast2-online-update-configuration`.

Por padrão, o download das atualizações é feito como RPMs delta. Como a reconstrução dos pacotes RPM com base nos RPMs delta é uma tarefa de alto consumo de memória e processador, certas instalações ou configurações de hardware podem exigir que você desabilite o uso de RPMs delta em benefício do desempenho.

Alguns patches, como atualizações do kernel ou pacotes que exigem contratos de licença, requerem a interação do usuário, o que pode parar o procedimento de atualização automática. É possível configurar para ignorar os patches que exigem interação do usuário.

PROCEDIMENTO 1.2 CONFIGURANDO A ATUALIZAÇÃO ONLINE AUTOMÁTICA

1. Após a instalação, inicie o YaST e selecione *Software* › *Configuração de Atualização Online*. Se preferir, inicie o módulo com `yast2 online_update_configuration` a partir da linha de comando.
2. Ative *Atualização Online Automática*.
3. Escolha o intervalo de atualização: *Diariamente*, *Semanalmente* ou *Mensalmente*.
4. Para aceitar automaticamente qualquer contrato de licença, ative *Agree with Licenses* (Concordar com Licenças).
5. Selecione se você deseja *Ignorar Patches Interativos* para que o procedimento de atualização continue até o fim automaticamente.

   Importante: Ignorando patches

   Se você ignorar qualquer pacote que exija interação, execute a *Atualização Online* manual de tempos em tempos para instalar também esses patches. Do contrário, você poderá perder patches importantes.

6. Para instalar automaticamente todos os pacotes recomendados por pacotes atualizados, ative *Incluir Pacotes Recomendados*.
7. Para desabilitar o uso de RPMs delta (por questões de desempenho), desative *Usar RPMs Delta*.
8. Para filtrar os patches por categoria (como segurança ou recomendado), ative *Filtrar por Categoria* e adicione as categorias de patch apropriadas da lista. Apenas os patches das categorias selecionadas serão instalados. Os outros serão ignorados.
9. Confirme sua configuração com *OK*.

2 Reunindo informações do sistema para suporte

Para uma rápida visão geral de todas as informações de sistema relevantes de uma máquina, o SUSE Linux Enterprise Desktop oferece o pacote `hostinfo`. Ele também ajuda os administradores do sistema a verificarem se há Kernels contaminados (que não são suportados) ou quaisquer pacotes de terceiros instalados na máquina.

Em caso de problemas, é possível criar um relatório detalhado do sistema com a ferramenta de linha de comando **`supportconfig`** ou o módulo de *Suporte* do YaST. Os dois coletam informações sobre o sistema, como a versão atual do kernel, o hardware, os pacotes instalados, a configuração da partição, etc. O resultado é um armazenamento de arquivos TAR. Após abrir uma Solicitação de Serviço (SS), você poderá fazer upload do armazenamento TAR para o Suporte Técnico Global. Ele ajuda a localizar o problema que você relatou e a orientá-lo para uma solução.

Você também pode verificar se há problemas conhecidos na saída do **`supportconfig`** para ajudar a resolvê-los mais rapidamente. Para esta finalidade, o SUSE Linux Enterprise Desktop oferece uma aplicação e uma ferramenta de linha de comando para `Supportconfig Analysis` (SCA).

2.1 Exibindo informações atuais do sistema

Para uma visão geral rápida e fácil de todas as informações do sistema relevantes, use o pacote `hostinfo` ao efetuar login no servidor. Após ser instalado na máquina, o console exibirá as seguintes informações para qualquer usuário `root` que efetuar login nessa máquina:

EXEMPLO 2.1 SAÍDA DE `hostinfo` AO EFETUAR LOGIN COMO `root`

```
Hostname:                earth
Current As Of:           Wed 12 Mar 2014 03:57:05 PM CET
Distribution:            SUSE Linux Enterprise Server 12
 -Service Pack:          0
Architecture:            x86_64
Kernel Version:          3.12.12-3-default
 -Installed:             Mon 10 Mar 2014 03:15:05 PM CET
 -Status:                Not Tainted
```

```
Last Updated Package:     Wed 12 Mar 2014 03:56:43 PM CET
 -Patches Needed:         0
 -Security:               0
 -3rd Party Packages:     0
IPv4 Address:             ens3 192.168.1.1
Total/Free/+Cache Memory: 983/95/383 MB (38% Free)
Hard Disk:                /dev/sda 10 GB
```

Caso a saída apresente o Kernel com status `tainted` (contaminado), consulte a *Seção 2.5, "Suporte aos módulos do Kernel"* para mais detalhes.

2.2 Coletando informações do sistema com o supportconfig

Para criar um armazenamento TAR com informações detalhadas do sistema que você possa enviar ao Suporte Técnico Global, use a ferramenta de linha de comando **`supportconfig`** diretamente ou o módulo de *Suporte* do YaST. A ferramenta de linha de comando está incluída no pacote `supportutils`, que é instalado por padrão. O módulo de *Suporte* do YaST também é baseado na ferramenta de linha de comando.

2.2.1 Criando um número de solicitação de serviço

É possível gerar armazenamentos do supportconfig a qualquer momento. No entanto, para enviar os dados do supportconfig ao Suporte Técnico Global, é necessário gerar primeiro um número de solicitação de serviço. Você precisa dele para fazer upload do armazenamento para o suporte.

Para criar uma solicitação de serviço, acesse http://www.novell.com/center/eservice e siga as instruções na tela. Anote o seu número de solicitação de serviço de 11 dígitos.

Nota: Declaração de Privacidade

A SUSE e a Novell tratam os relatórios do sistema como dados confidenciais. Para ver detalhes do nosso compromisso de privacidade, acesse http://www.novell.com/company/legal/privacy/.

2.2.2 Destinos de upload

Após criar um número de solicitação de serviço, você poderá fazer upload dos armazenamentos supportconfig para o Suporte Técnico Global, conforme descrito no *Procedimento 2.1, "Submetendo informações ao suporte com o YaST"* ou no *Procedimento 2.2, "Submetendo informações ao suporte por linha de comando"*. Use um dos seguintes destinos de upload:

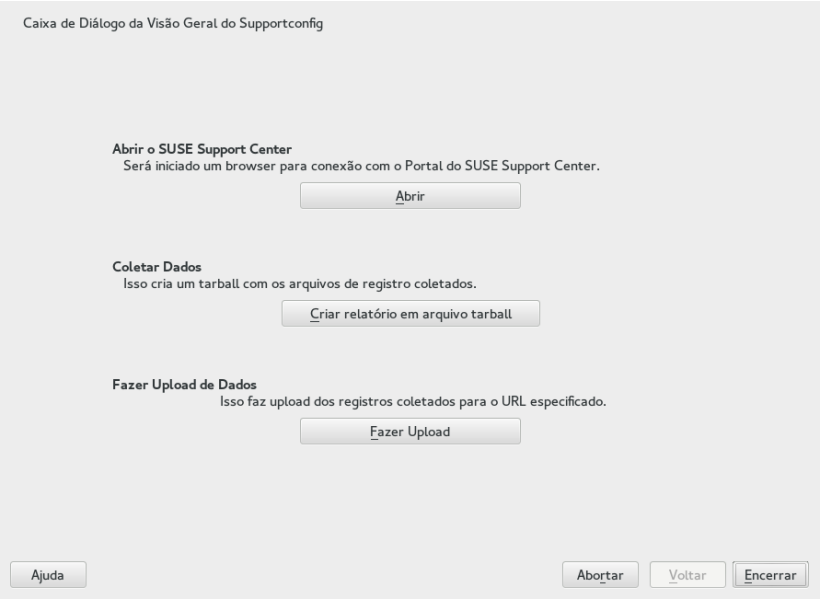
- Clientes nos EUA: ftp://ftp.novell.com/incoming
- EMEA, Europa, Oriente Médio e África: ftp://support-ftp.suse.com/in

Você também pode anexar o armazenamento TAR manualmente à sua solicitação de serviço usando o URL da solicitação de serviço: http://www.novell.com/center/eservice.

2.2.3 Criando um armazenamento supportconfig com o YaST

Para usar o YaST para coletar informações do sistema, faça o seguinte:

1. Inicie o YaST e abra o módulo de *Suporte*.


Caixa de Diálogo da Visão Geral do Supportconfig
Abrir o SUSE Support Center
Será iniciado um browser para conexão com o Portal do SUSE Support Center.
Abrir
Coletar Dados
Isso cria um tarball com os arquivos de registro coletados.
Criar relatório em arquivo tarball
Fazer Upload de Dados
Isso faz upload dos registros coletados para o URL especificado.
Fazer Upload
Ajuda
Abortar
Voltar
Encerrar

2. Clique em *Criar relatório em arquivo tarball*.

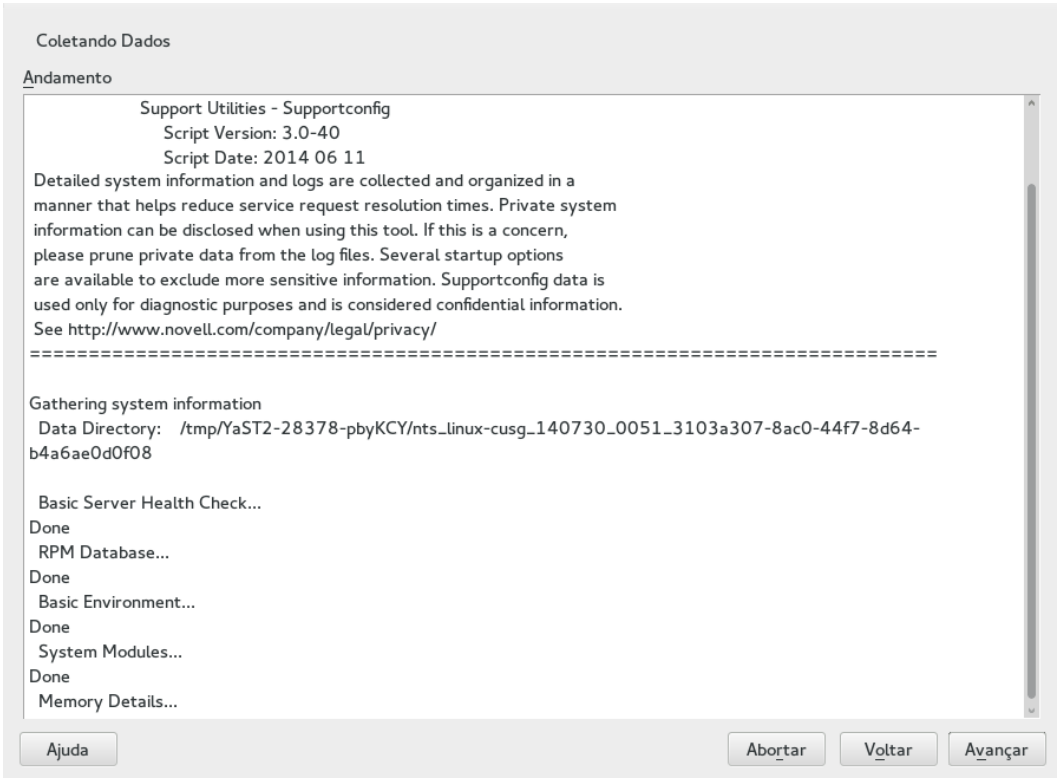
3. Na janela seguinte, selecione uma das opções de supportconfig na lista de botões de opção. Por padrão, a opção *Usar Configurações (Técnicas) Personalizadas* está pré-selecionada. Para testar primeiro a função de relatório, use *Reunir apenas uma quantidade mínima de informações*. Para obter algumas informações básicas sobre outras opções, consulte a página de manual de **`supportconfig`**.
   Continue com *Avançar*.

4. Digite suas informações de contato. Elas são gravadas em um arquivo chamado `basic-environment.txt` e incluídas no armazenamento que será criado.

5. Para submeter o armazenamento ao Suporte Técnico Global no fim do processo de coleta de informações, a opção *Informações de Upload* é obrigatória. O YaST propõe um servidor de upload automaticamente. Para modificá-lo, consulte a *Seção 2.2.2, "Destinos de upload"* para saber os detalhes de quais servidores de upload estão disponíveis.
   Para submeter o armazenamento mais tarde, deixe a opção *Informações de Upload* vazia por enquanto.

6. Continue com *Avançar*.

7. A coleta de informações é iniciada.


Coletando Dados
Andamento
Support Utilities - Supportconfig
Script Version: 3.0-40
Script Date: 2014 06 11
Detailed system information and logs are collected and organized in a
manner that helps reduce service request resolution times. Private system
information can be disclosed when using this tool. If this is a concern,
please prune private data from the log files. Several startup options
are available to exclude more sensitive information. Supportconfig data is
used only for diagnostic purposes and is considered confidential information.
See http://www.novell.com/company/legal/privacy/
Gathering system information
Data Directory: /tmp/YaST2-28378-pbyKCY/nts_linux-cusg_140730_0051_3103a307-8ac0-44f7-8d64-b4a6ae0d0f08
Basic Server Health Check...
Done
RPM Database...
Done
Basic Environment...
Done
System Modules...
Done
Memory Details...
Ajuda
Abortar
Voltar
Avançar

Quando o processo for concluído, continue com *Avançar*.

8. Revise a coleta de dados: Selecione o *Nome do Arquivo* de um registro para ver seu conteúdo no YaST. Para remover arquivos do armazenamento TAR antes de submetê-lo ao suporte, use *Remover dos Dados*. Continue com *Avançar*.

9. Grave o armazenamento TAR. Se você iniciar o módulo do YaST como usuário `root`, por padrão, o YaST vai propor gravar o armazenamento em `/var/log` (ou em seu diretório pessoal). O formato do nome de arquivo é `nts_HOST_DATA_HORÁRIO.tbz`.

10. Para fazer upload do armazenamento diretamente para o suporte, verifique se a opção *Fazer upload do tarball com arquivos de registro para o URL* está ativada. O *Destino do Upload* mostrado aqui é aquele proposto pelo YaST no *Passo 5*. Para modificar o destino do upload, encontre as informações detalhadas sobre quais servidores de upload estão disponíveis na *Seção 2.2.2, "Destinos de upload"*.

11. Para ignorar o upload, desative a opção *Fazer upload do tarball com arquivos de registro para o URL*.

12. Confirme as mudanças para fechar o módulo do YaST.

2.2.4 Criando um armazenamento supportconfig da linha de comando

O seguinte procedimento mostra como criar um armazenamento supportconfig, mas sem o submeter diretamente ao suporte. Para fazer seu upload, é necessário executar o comando com algumas opções, conforme descrito no *Procedimento 2.2, "Submetendo informações ao suporte por linha de comando"*.

1. Abra um shell e torne-se `root`.

2. Execute **`supportconfig`** sem qualquer opção. Isso reúne as informações padrão do sistema.

3. Aguarde a ferramenta concluir a operação.

4. O local padrão do armazenamento é `/var/log`, com o formato de nome de arquivo `nts_HOST_DATA_HORÁRIO.tbz`

2.2.5 Opções comuns do supportconfig

O utilitário **supportconfig** é geralmente chamado sem nenhuma opção. Exiba uma lista de todas as opções com **supportconfig** `-h` ou consulte a página de manual. A seguinte lista apresenta uma breve visão geral de alguns casos de uso comuns:

Reduzindo o Tamanho das Informações Coletadas

Usar a opção mínima (`-m`):

```
supportconfig -m
```

Limitando as Informações a Determinado Tópico

Se você já localizou um problema com a saída padrão do **supportconfig** e descobriu que ele está relacionado apenas a determinada área ou conjunto de recursos, convém limitar as informações coletadas à área especifica na próxima execução do **supportconfig**. Por exemplo, se você detectar problemas com o LVM e quiser testar uma recente mudança feita na configuração do LVM, convém coletar o mínimo de informações do supportconfig apenas sobre o LVM:

```
supportconfig -i LVM
```

Para ver a lista completa de palavras-chave de recursos que você pode usar para limitar as informações coletadas a determinada área, execute

```
supportconfig -F
```

Incluindo Informações de Contato Adicionais na Saída:

```
supportconfig -E tux@example.org -N "Tux Penguin" -O "Penguin Inc." ...
```

(tudo em uma linha)

Coletando Arquivos de Registro Já Rotacionados

```
supportconfig -l
```

Isso é útil principalmente em ambientes de alto registro ou após uma falha do kernel quando o syslog gira os arquivos de registro após uma reinicialização.

2.3 Submetendo informações ao suporte técnico global

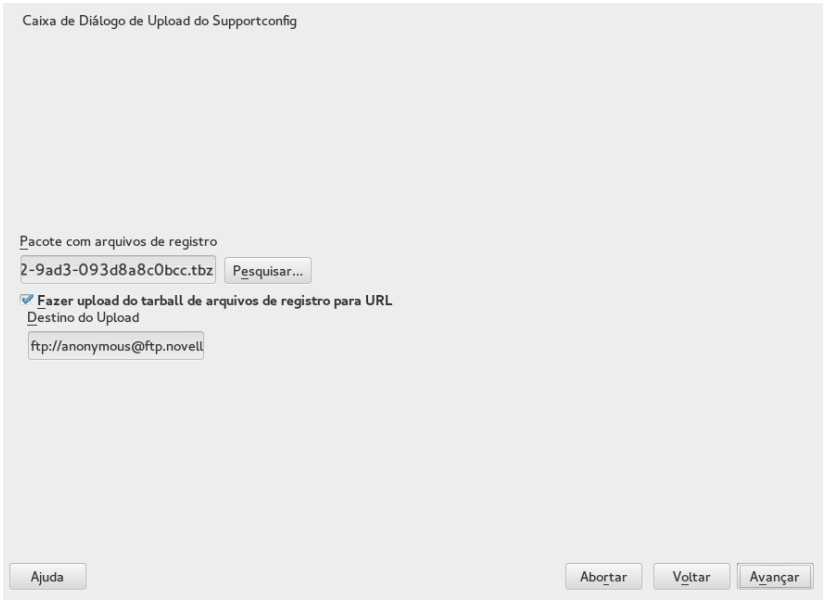
Use o módulo de *Suporte* do YaST ou o utilitário de linha de comando **supportconfig** para submeter as informações do sistema ao Suporte Técnico Global. Se você tiver um problema com o servidor e quiser a ajuda do suporte, precisará abrir primeiro uma solicitação de serviço. Para obter os detalhes, consulte a *Seção 2.2.1, "Criando um número de solicitação de serviço"*.

Os seguintes exemplos usam *12345678901* como marcador para o número da sua solicitação de serviço. Substitua *12345678901* pelo número da solicitação de serviço que você criou na *Seção 2.2.1, "Criando um número de solicitação de serviço"*.

PROCEDIMENTO 2.1 SUBMETENDO INFORMAÇÕES AO SUPORTE COM O YAST

O seguinte procedimento considera que você já tenha criado um armazenamento supportconfig, mas ainda não tenha feito upload dele. Verifique se você incluiu suas informações de contato no armazenamento, conforme descrito na *Seção 2.2.3, "Criando um armazenamento supportconfig com o YaST", Passo 4*. Para ver instruções de como gerar e submeter de uma só vez um armazenamento supportconfig, consulte a *Seção 2.2.3, "Criando um armazenamento supportconfig com o YaST"*.

1. Inicie o YaST e abra o módulo de *Suporte*.
2. Clique em *Fazer Upload*.
3. Em *Pacote com arquivos de registro*, especifique o caminho para o armazenamento supportconfig existente ou use *Pesquisar*.
4. O YaST propõe um servidor de upload automaticamente. Para modificá-lo, consulte a *Seção 2.2.2, "Destinos de upload"* para saber os detalhes de quais servidores de upload estão disponíveis.



Continue com *Avançar*.

5. Clique em *Concluir*.

PROCEDIMENTO 2.2 SUBMETENDO INFORMAÇÕES AO SUPORTE POR LINHA DE COMANDO

O seguinte procedimento considera que você já tenha criado um armazenamento supportconfig, mas ainda não tenha feito upload dele. Para ver instruções de como gerar e submeter de uma só vez um armazenamento supportconfig, consulte a *Seção 2.2.3, "Criando um armazenamento supportconfig com o YaST"*.

1. Servidores com conectividade à Internet:

   a. Para usar o destino de upload padrão, execute:

   ```
   supportconfig -ur 12345678901
   ```

   b. Para o destino de upload seguro, use o seguinte:

   ```
   supportconfig -ar 12345678901
   ```

2. Servidores *sem* conectividade à Internet

   a. Execute o seguinte:

   ```
   supportconfig -r 12345678901
   ```

b. Faça upload do armazenamento `/var/log/nts_SR12345678901*tbz` manualmente para um de nossos servidores FTP. O servidor que deverá ser usado depende da sua localização global. Para uma visão geral, consulte a *Seção 2.2.2, "Destinos de upload"*.

3. Depois que o armazenamento TAR estiver no diretório de entrada do nosso servidor FTP, ele será automaticamente anexado à sua solicitação de serviço.

2.4 Analisando informações do sistema

É possível analisar os relatórios do sistema criados com o **`supportconfig`** para ver se há problemas conhecidos e agilizar sua solução. Para esta finalidade, o SUSE Linux Enterprise Desktop oferece uma aplicação e uma ferramenta de linha de comando para `Supportconfig Analysis` (SCA). A aplicação SCA é uma ferramenta não interativa executada no servidor. A ferramenta SCA (**`scatool`**) é executada no cliente por linha de comando. As duas ferramentas analisam os armazenamentos supportconfig dos servidores afetados. A análise inicial do servidor ocorre na aplicação SCA ou na estação de trabalho em que a scatool é executada. Nenhum ciclo de análise é realizado no servidor de produção.

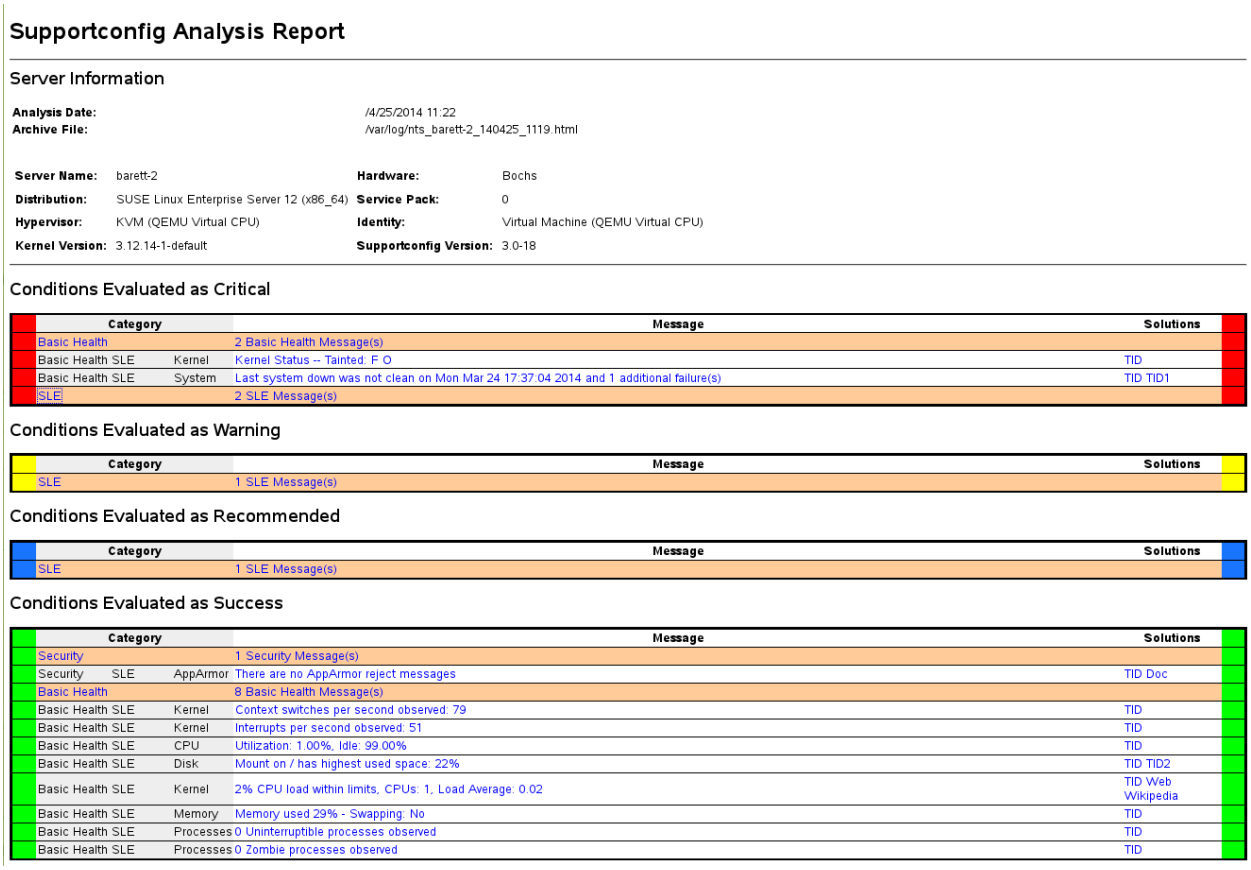
Tanto a aplicação quanto a ferramenta de linha de comando também precisam de padrões específicos do produto, que as permitem analisar a saída do supportconfig dos produtos associados. Cada padrão é um script que analisa e avalia um armazenamento supportconfig referente a um problema conhecido. Os padrões estão disponíveis como pacotes RPM.

Por exemplo, para analisar armazenamentos supportconfig que foram gerados em uma máquina com o SUSE Linux Enterprise 11, é necessário instalar o pacote `sca-patterns-sle11` juntamente com a ferramenta SCA (ou na máquina que deseja usar como servidor da aplicação SCA). Para analisar armazenamentos supportconfig gerados em uma máquina com o SUSE Linux Enterprise 10, o pacote `sca-patterns-sle10` é necessário.

É possível também desenvolver seus próprios padrões, conforme descrito resumidamente na *Seção 2.4.3, "Desenvolvendo padrões de análise personalizados"*.

2.4.1 Ferramenta de linha de comando SCA

A ferramenta de linha de comando SCA permite analisar uma máquina local usando o **`supportconfig`** e os padrões de análise referentes ao produto específico que está instalado na máquina local. A ferramenta cria um relatório HTML que mostra os resultados da análise. Para obter um exemplo, consulte a *Figura 2.1, "Relatório HTML gerado pela ferramenta SCA"*.



Supportconfig Analysis Report

Server Information

Analysis Date: /4/25/2014 11:22
Archive File: /var/log/nts_barett-2_140425_1119.html

Server Name:	barett-2	**Hardware:**	Bochs
Distribution:	SUSE Linux Enterprise Server 12 (x86_64)	**Service Pack:**	0
Hypervisor:	KVM (QEMU Virtual CPU)	**Identity:**	Virtual Machine (QEMU Virtual CPU)
Kernel Version:	3.12.14-1-default	**Supportconfig Version:**	3.0-18

Conditions Evaluated as Critical

Category			Message	Solutions
Basic Health			2 Basic Health Message(s)	
Basic Health	SLE	Kernel	Kernel Status -- Tainted: F O	TID
Basic Health	SLE	System	Last system down was not clean on Mon Mar 24 17:37:04 2014 and 1 additional failure(s)	TID TID1
SLE			2 SLE Message(s)	

Conditions Evaluated as Warning

Category	Message	Solutions
SLE	1 SLE Message(s)	

Conditions Evaluated as Recommended

Category	Message	Solutions
SLE	1 SLE Message(s)	

Conditions Evaluated as Success

Category			Message	Solutions
Security			1 Security Message(s)	
Security	SLE	AppArmor	There are no AppArmor reject messages	TID Doc
Basic Health			8 Basic Health Message(s)	
Basic Health	SLE	Kernel	Context switches per second observed: 79	TID
Basic Health	SLE	Kernel	Interrupts per second observed: 51	TID
Basic Health	SLE	CPU	Utilization: 1.00%, Idle: 99.00%	TID
Basic Health	SLE	Disk	Mount on / has highest used space: 22%	TID TID2
Basic Health	SLE	Kernel	2% CPU load within limits, CPUs: 1, Load Average: 0.02	TID Web Wikipedia
Basic Health	SLE	Memory	Memory used 29% - Swapping: No	TID
Basic Health	SLE	Processes	0 Uninterruptible processes observed	TID
Basic Health	SLE	Processes	0 Zombie processes observed	TID

FIGURA 2.1 RELATÓRIO HTML GERADO PELA FERRAMENTA SCA

O comando **`scatool`** está incluído no pacote `sca-server-report`. Ele não é instalado por padrão. Você também precisa do pacote `sca-patterns-base` e de qualquer um dos pacotes `sca-patterns-*` específicos do produto correspondentes ao produto instalado na máquina em que deseja executar o comando **`scatool`**.

Execute o comando **`scatool`** como usuário `root` ou com **`sudo`**. Ao chamar a ferramenta SCA, é possível analisar um armazenamento TAR **`supportconfig`** existente ou deixar que ela gere e analise um novo armazenamento de uma vez. A ferramenta também oferece um console interativo (com preenchimento de tabulação) e a possibilidade de executar o **`supportconfig`** em uma máquina externa e de executar as análises subsequentes na máquina local.

Veja a seguir alguns exemplos de comandos:

`sudo scatool -s`

Chama o **`supportconfig`** e gera um novo armazenamento supportconfig na máquina local. Analisa o armazenamento para ver se há problemas conhecidos aplicando os padrões de análise da SCA correspondentes ao produto instalado. Exibe o caminho para o relatório HTML que é gerado com base nos resultados da análise. Normalmente, ele é gravado no mesmo diretório do armazenamento supportconfig.

`sudo scatool -s -o /opt/sca/reports/`

Igual ao **`sudo scatool -s`**, só que o relatório HTML é gravado no caminho especificado com `-o`.

`sudo scatool -a CAMINHO_PARA_TARBALL_OU_DIR`

Analisa o arquivo de armazenamento supportconfig especificado (ou o diretório indicado no qual o armazenamento supportconfig foi extraído). O relatório HTML gerado é gravado no mesmo local do armazenamento ou diretório do supportconfig.

`sudo scatool -a servidor_sles.empresa.com`

Estabelece uma conexão SSH com o servidor externo *`servidor_sles.empresa.com`* e executa o **`supportconfig`** no servidor. Em seguida, o armazenamento supportconfig é copiado novamente na máquina local e analisado nela. O relatório HTML gerado é gravado no diretório padrão `/var/log`. (Apenas o armazenamento supportconfig é criado em *`servidor_sles.empresa.com`*).

`sudo scatool -c`

Inicia o console interativo da **`scatool`**. Pressione →| duas vezes para ver os comandos disponíveis.

Para mais opções e informações, execute **`sudo scatool -h`** ou consulte a página de manual de **`scatool`**.

2.4.2 Aplicação SCA

Se você usar a aplicação SCA para analisar armazenamentos supportconfig, precisará configurar um servidor dedicado (ou máquina virtual) como servidor da aplicação SCA. Depois disso, o servidor da aplicação SCA poderá ser usado para analisar armazenamentos supportconfig em todas as máquinas da sua empresa que tenham o SUSE Linux Enterprise Server ou o SUSE Linux

Enterprise Desktop. Basta fazer upload dos armazenamentos supportconfig para o servidor da aplicação para análise. Não é necessária nenhuma interação. Em um banco de dados MariaDB, a aplicação SCA monitora todos os armazenamentos supportconfig que foram analisados. É possível ler os relatórios da SCA diretamente da interface da Web da aplicação. Se você preferir, a aplicação poderá enviar o relatório HTML por e-mail para qualquer usuário administrativo. Para obter os detalhes, consulte a *Seção 2.4.2.5.4, "Enviando relatórios da SCA por e-mail"*.

Para instalar e configurar rapidamente a aplicação SCA por linha de comando, siga as instruções na *Seção 2.4.2.1, "Inicialização Rápida da Instalação"*. O procedimento é para especialistas e está centrado na instalação limpa e nos comandos de configuração. Para obter mais informações, consulte a descrição mais detalhada da *Seção 2.4.2.2, "Pré-requisitos"* até a *Seção 2.4.2.3, "Instalação e configuração básica"*.

2.4.2.1 Inicialização Rápida da Instalação

PRÉ-REQUISITOS

- Padrão da Web e LAMP
- Módulo da Web e de Criação de Scripts (você deve registrar a máquina para selecionar esse módulo).

Nota: Privilégios de `root` necessários

Todos os comandos do procedimento a seguir devem ser executados como `root`.

PROCEDIMENTO 2.3 INSTALAÇÃO USANDO FTP ANÔNIMO PARA UPLOAD

Depois que a aplicação estiver funcionando, não será necessária mais nenhuma interação manual. Portanto, esta forma de configurar a aplicação é ideal ao usar tarefas cron para criar e fazer upload de armazenamentos supportconfig.

1. Na máquina de instalação da aplicação, efetue login no console e execute os seguintes comandos:

```
zypper install sca-appliance-* sca-patterns-* vsftpd
systemctl enable apache2.service
systemctl start apache2.service
systemctl enable vsftpd.service
```

```
systemctl start vsftpd.service
yast ftp-server
```

2. No Servidor FTP do YaST, selecione *Autenticação* › *Habilitar Upload* › *Anônimo Pode Fazer Upload* › *Concluir* › *Sim* para *Criar /srv/ftp/upload*.

3. Execute os seguintes comandos:

```
systemctl enable mysql.service
systemctl start mysql.service
mysql_secure_installation
setup-sca -f
```

A mysql_secure_installation cria uma senha de `root` do MariaDB.

PROCEDIMENTO 2.4 INSTALAÇÃO USANDO SCP/TMP PARA UPLOAD

Esta forma de configurar a aplicação requer interação manual para digitar a senha SSH.

1. Na máquina de instalação da aplicação, efetue login no console.

2. Execute os seguintes comandos:

```
zypper install sca-appliance-* sca-patterns-*
systemctl enable apache2.service
systemctl start apache2.service
sudo systemctl enable mysql.service
systemctl start mysql.service
mysql_secure_installation
setup-sca
```

2.4.2.2 Pré-requisitos

Para executar um servidor da aplicação SCA, são necessários os seguintes pré-requisitos:

- Todos os pacotes `sca-appliance-*`.
- O pacote `sca-patterns-base`. Adicionalmente, qualquer um dos `sca-patterns-*` específicos do produto, de acordo com o tipo de armazenamento supportconfig que você deseja analisar com a aplicação.

- Apache
- PHP
- MariaDB
- Servidor FTP anônimo (opcional)

2.4.2.3 Instalação e configuração básica

Conforme listado na *Seção 2.4.2.2, "Pré-requisitos"*, a aplicação SCA possui várias dependências em outros pacotes. Portanto, você precisa fazer algumas preparações antes de instalar e configurar o servidor da aplicação SCA:

1. No Apache e no MariaDB, instale os padrões de instalação da `Web` e `LAMP`.
2. Configure o Apache, o MariaDB e, opcionalmente, um servidor FTP anônimo.
3. Configure o Apache e o MariaDB para iniciarem no momento da inicialização:

   ```
   sudo systemctl enable apache2.service mysql.service
   ```

4. Inicie os dois serviços:

   ```
   sudo systemctl start apache2.service mysql.service
   ```

Agora você pode instalar a aplicação SCA e configurá-la conforme descrito no *Procedimento 2.5, "Instalando e configurando a aplicação SCA"*.

PROCEDIMENTO 2.5 INSTALANDO E CONFIGURANDO A APLICAÇÃO SCA

Após instalar os pacotes, use o script **`setup-sca`** para a configuração básica do banco de dados de administração e relatório MariaDB, que é usado pela aplicação SCA.

Ele pode ser usado para configurar as seguintes opções disponíveis para fazer upload dos armazenamentos supportconfig de suas máquinas para a aplicação SCA:

- **`scp`**
- servidor FTP anônimo

1. Instale a aplicação e a biblioteca de padrões com base na SCA:

```
sudo zypper install sca-appliance-* sca-patterns-base
```

2. Instale também os pacotes de padrões de acordo com os tipos de armazenamentos supportconfig que você deseja analisar. Por exemplo, se você tem servidores SUSE Linux Enterprise Server 11 e SUSE Linux Enterprise Server 12 em seu ambiente, instale os dois pacotes `sca-patterns-sle11` e `sca-patterns-sle12`.
   Para instalar todos os padrões disponíveis:

```
zypper install sca-patterns-*
```

3. Para a configuração básica da aplicação SCA, use o script **`setup-sca`**. O modo como ele é chamado depende de como você deseja fazer upload dos armazenamentos supportconfig para o servidor da aplicação SCA:

   - Se você configurar um servidor FTP anônimo que usa o diretório `/srv/ftp/upload`, execute o script de configuração com a opção `-f` e siga as instruções na tela:

     ```
     setup-sca -f
     ```

     Nota: Servidor FTP que usa outro diretório

     Se o seu servidor FTP usa um diretório diferente do `/srv/ftp/upload`, ajuste os seguintes arquivos de configuração para apontarem para o diretório correto: `/etc/sca/sdagent.conf` e `/etc/sca/sdbroker.conf` .

   - Para fazer upload dos arquivos supportconfig para o diretório `/tmp` do servidor da aplicação SCA usando o comando **`scp`**, chame o script de configuração sem nenhum parâmetro e siga as instruções na tela:

     ```
     setup-sca
     ```

   O script de configuração executa algumas verificações referentes a seus requisitos e configura os subcomponentes necessários. Ele pede duas senhas: a senha de `root` MySQL do MariaDB que você configurou e uma senha de usuário da Web usada para efetuar login na interface da Web da aplicação SCA.

4. Digite a senha de `root` existente do MariaDB. Isso permite que a aplicação SCA se conecte com o MariaDB.

5. Defina uma senha para o usuário da Web. Ela será gravada em `/srv/www/htdocs/sca/web-config.php` e definida como a senha do usuário `scdiag`. Tanto o nome de usuário quanto a senha podem ser mudados a qualquer momento. Consulte a *Seção 2.4.2.5.1, "Senha da interface da Web"*.

Após a instalação e configuração bem-sucedidas, a aplicação SCA estará pronta para uso. Consulte a *Seção 2.4.2.4, "Usando a aplicação SCA"*. No entanto, é possível modificar algumas opções, como mudar a senha da interface da Web, mudar a fonte das atualizações dos padrões da SCA, habilitar o modo de arquivamento ou configurar notificações por e-mail. Para ver os detalhes sobre isso, consulte a *Seção 2.4.2.5, "Personalizando a aplicação SCA"*.

Atenção: Proteção de Dados

Como os relatórios no servidor da aplicação SCA incluem informações relacionadas à segurança sobre as máquinas em que os armazenamentos supportconfig foram analisados, proteja os dados do servidor da aplicação SCA contra acesso não autorizado.

2.4.2.4 Usando a aplicação SCA

É possível fazer upload dos armazenamentos supportconfig existentes para a aplicação SCA manualmente ou criar novos armazenamentos supportconfig e fazer upload deles para a aplicação SCA em uma etapa. O upload pode ser feito por FTP ou SCP. Nos dois, é necessário saber o URL para acessar a aplicação SCA. Para upload por FTP, um servidor FTP precisa ser configurado para a aplicação SCA. Consulte o *Procedimento 2.5, "Instalando e configurando a aplicação SCA"*.

2.4.2.4.1 Fazendo upload de armazenamentos supportconfig para a aplicação SCA

- Para criar um armazenamento supportconfig e fazer seu upload por FTP (anônimo):

```
sudo supportconfig -U "ftp://sca-appliance.company.com/upload"
```

- Para criar um armazenamento supportconfig e fazer seu upload por SCP:

```
sudo supportconfig -U “scp://sca-appliance.company.com/tmp”
```

Você deverá informar a senha de usuário `root` do servidor que executa a aplicação SCA.

- Para fazer upload de um ou vários armazenamentos manualmente, copie os arquivos de armazenamento existentes (normalmente em `/var/log/nts_*.tbz`) para a aplicação SCA. Como destino, use o diretório `/tmp` do servidor da aplicação ou o diretório `/srv/ftp/upload` (se FTP estiver configurado para o servidor da aplicação SCA).

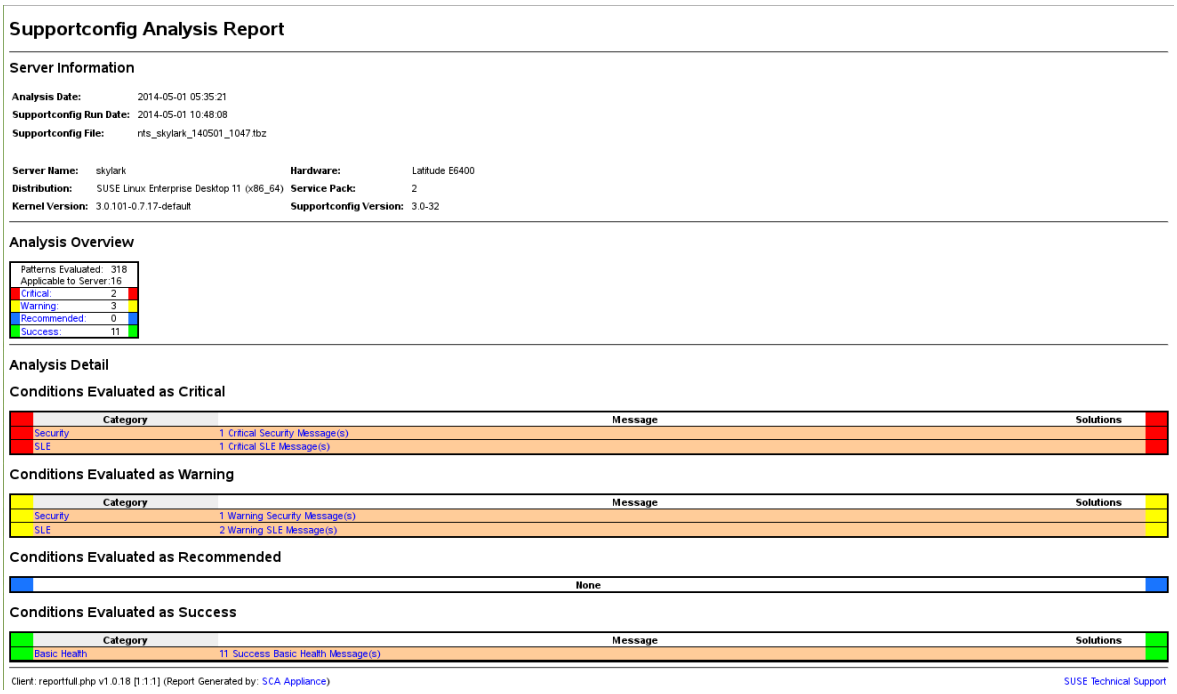
2.4.2.4.2 Vendo relatórios da SCA

É possível ver os relatórios da SCA de qualquer máquina que tenha um browser instalado e acesso à página de índice de relatórios da aplicação SCA.

1. Inicie o browser da Web e verifique se o JavaScript e os cookies estão habilitados.
2. Como URL, insira a página de índice de relatórios da aplicação SCA.

   ```
   https://sca-appliance.company.com/sca
   ```

   Se estiver em dúvida, pergunte ao administrador do sistema.
3. Você deverá informar o nome de usuário e a senha para efetuar login.



Supportconfig Analysis Report

Server Information

Analysis Date: 2014-05-01 05:35:21
Supportconfig Run Date: 2014-05-01 10:48:08
Supportconfig File: nts_skylark_140501_1047.tbz

Server Name: skylark
Distribution: SUSE Linux Enterprise Desktop 11 (x86_64)
Kernel Version: 3.0.101-0.7.17-default
Hardware: Latitude E6400
Service Pack: 2
Supportconfig Version: 3.0-32

Analysis Overview

Patterns Evaluated:	318
Applicable to Server:	16
Critical:	2
Warning:	3
Recommended:	0
Success:	11

Analysis Detail

Conditions Evaluated as Critical

Category	Message	Solutions
Security	1 Critical Security Message(s)	
SLE	1 Critical SLE Message(s)	

Conditions Evaluated as Warning

Category	Message	Solutions
Security	1 Warning Security Message(s)	
SLE	2 Warning SLE Message(s)	

Conditions Evaluated as Recommended

None

Conditions Evaluated as Success

Category	Message	Solutions
Basic Health	11 Success Basic Health Message(s)	

Client: reportfull.php v1.0.18 [1.1.1] (Report Generated by: SCA Appliance) SUSE Technical Support

FIGURA 2.2 RELATÓRIO HTML GERADO PELA APLICAÇÃO SCA

4. Após o login, clique na data do relatório que deseja ler.
5. Clique primeiro na categoria *Basic Health* (Saúde Básica) para expandi-la.
6. Na coluna *Message* (Mensagem), clique em uma entrada. O artigo correspondente é aberto no SUSE Knowledgebase. Leia a solução proposta e siga as instruções.
7. Se a coluna *Solutions* (Soluções) do *Relatório da Supportconfig Analysis* mostrar qualquer outra entrada, clique nela. Leia a solução proposta e siga as instruções.
8. Consulte o SUSE Knowledgebase (http://www.suse.com/support/kb/) para ver resultados diretamente relacionados ao problema identificado pela SCA. Resolva o problema.
9. Procure resultados que possam ser usados proativamente para evitar futuros problemas.

2.4.2.5 Personalizando a aplicação SCA

As seguintes seções mostram como mudar a senha da interface da Web, como mudar a fonte das atualizações dos padrões da SCA, como habilitar o modo de arquivamento e como configurar notificações por e-mail.

2.4.2.5.1 Senha da interface da Web

A interface da Web da aplicação SCA requer nome de usuário e senha para login. O nome de usuário padrão é `scdiag` e a senha padrão é `linux` (caso não tenham sido especificados de outra forma. Consulte o *Procedimento 2.5, "Instalando e configurando a aplicação SCA"*). Mude a senha padrão para uma senha segura na primeira oportunidade. É possível também modificar o nome de usuário.

PROCEDIMENTO 2.6 MUDANDO NOME DE USUÁRIO OU SENHA DA INTERFACE DA WEB

1. Efetue login como usuário `root` no console do sistema do servidor da aplicação SCA.
2. Abra o `/srv/www/htdocs/sca/web-config.php` em um editor.
3. Mude os valores de `$username` e `$password` conforme desejado.
4. Grave o arquivo e saia.

2.4.2.5.2 Atualizações dos padrões da SCA

Por padrão, todos os pacotes `sca-patterns-*` são atualizados regularmente por uma tarefa cron `root` que executa o script `sdagent-patterns` durante a noite, que, por sua vez, executa **`zypper update sca-patterns-*`**. Uma atualização regular de sistema atualiza todos os pacotes de padrões e da aplicação SCA. Para atualizar a aplicação SCA e os padrões manualmente, execute:

```
sudo zypper update sca-*
```

Por padrão, as atualizações são instaladas do repositório de atualização do SUSE Linux Enterprise 12. Você poderá mudar a fonte das atualizações para um servidor SMT, se desejado. Quando `sdagent-patterns` executa **`zypper update sca-patterns-*`**, ele acessa as atualizações do canal de atualização configurado no momento. Se esse canal estiver em um servidor SMT, os pacotes serão acessados de lá.

PROCEDIMENTO 2.7 DESABILITANDO ATUALIZAÇÕES AUTOMÁTICAS DE PADRÕES DA SCA

1. Efetue login como usuário `root` no console do sistema do servidor da aplicação SCA.
2. Abra o `/etc/sca/sdagent-patterns.conf` em um editor.

3. Mudar a entrada

```
UPDATE_FROM_PATTERN_REPO=1
```

para

```
UPDATE_FROM_PATTERN_REPO=0
```

4. Grave o arquivo e saia. Não é necessário reiniciar a máquina para aplicar a mudança.

2.4.2.5.3 Modo de arquivamento

Todos os armazenamentos supportconfig serão apagados da aplicação SCA depois de serem analisados e de seus resultados serem armazenados no banco de dados MariaDB. Para fins de solução de problemas, no entanto, convém manter cópias dos armazenamentos supportconfig da máquina. Por padrão, o modo de arquivamento está desabilitado.

PROCEDIMENTO 2.8 HABILITANDO O MODO DE ARQUIVAMENTO NA APLICAÇÃO SCA

1. Efetue login como usuário `root` no console do sistema do servidor da aplicação SCA.
2. Abra o `/etc/sca/sdagent.conf` em um editor.
3. Mudar a entrada

```
ARCHIVE_MODE=0
```

para

```
ARCHIVE_MODE=1
```

4. Grave o arquivo e saia. Não é necessário reiniciar a máquina para aplicar a mudança.

Após habilitar o modo de arquivamento, a aplicação SCA gravará os arquivos supportconfig no diretório `/var/log/archives/saved`, em vez de apagá-los.

2.4.2.5.4 Enviando relatórios da SCA por e-mail

A aplicação SCA pode enviar um arquivo HTML de relatório por e-mail referente a cada supportconfig analisado. Por padrão, este recurso está desabilitado. Ao habilitá-lo, é possível definir uma lista de endereços de e-mail para os quais enviar os relatórios e especificar um nível de mensagens de status que aciona o envio dos relatórios (`STATUS_NOTIFY_LEVEL`).

VALORES POSSÍVEIS PARA `STATUS_NOTIFY_LEVEL`

$STATUS_OFF

Desativar o envio de relatórios HTML.

$STATUS_CRITICAL

Enviar apenas relatórios da SCA que incluam CRITICAL (Crítico).

$STATUS_WARNING

Enviar apenas relatórios da SCA que incluam WARNING (Aviso) ou CRITICAL.

$STATUS_RECOMMEND

Enviar apenas relatórios da SCA que incluam RECOMMEND (Recomendado), WARNING ou CRITICAL.

$STATUS_SUCCESS

Enviar relatórios da SCA que incluam SUCCESS (Êxito), RECOMMEND, WARNING ou CRITICAL.

PROCEDIMENTO 2.9 CONFIGURANDO NOTIFICAÇÕES POR E-MAIL PARA RELATÓRIOS DA SCA

1. Efetue login como usuário `root` no console do sistema do servidor da aplicação SCA.
2. Abra o `/etc/sca/sdagent.conf` em um editor.
3. Pesquise a entrada `STATUS_NOTIFY_LEVEL`. Por padrão, ela está definida como `$STATUS_OFF` (notificações por e-mail desabilitadas).
4. Para habilitar as notificações por e-mail, mude `$STATUS_OFF` para o nível de mensagens de status para o qual deseja gerar relatórios por e-mail, por exemplo:

   ```
   STATUS_NOTIFY_LEVEL=$STATUS_SUCCESS
   ```

   Para obter os detalhes, consulte *Valores possíveis para* `STATUS_NOTIFY_LEVEL`.
5. Para definir a lista de destinatários que devem receber os relatórios:

a. Pesquise a entrada `EMAIL_REPORT='root'`.

b. Substitua `root` pela lista de endereços de e-mail aos quais enviar os relatórios da SCA. Os endereços de e-mail devem ser separados por espaços. Por exemplo:

```
EMAIL_REPORT='tux@my.company.com wilber@your.company.com'
```

6. Grave o arquivo e saia. Não é necessário reiniciar a máquina para aplicar as mudanças. Todos os relatórios futuros da SCA serão enviados por e-mail aos endereços especificados.

2.4.2.6 Fazendo backup e restaurando o banco de dados

Para fazer backup e restaurar o banco de dados MariaDB que armazena os relatórios da SCA, use o comando **`scadb`**, conforme descrito a seguir.

PROCEDIMENTO 2.10 FAZENDO BACKUP DO BANCO DE DADOS

1. Efetue login como usuário `root` no console do sistema do servidor que executa a aplicação SCA.
2. Coloque a aplicação no modo de manutenção executando:

```
scadb maint
```

3. Inicie o backup com:

```
scadb backup
```

   Os dados são gravados em um armazenamento TAR: `sca-backup-*sql.gz`.

4. Se você usa o banco de dados de criação de padrões para desenvolver seus próprios padrões (consulte a *Seção 2.4.3, "Desenvolvendo padrões de análise personalizados"*), faça backup também destes dados:

```
sdpdb backup
```

   Os dados são gravados em um armazenamento TAR: `sdp-backup-*sql.gz`.

5. Copie os seguintes dados para outra máquina ou para um meio de armazenamento externo:

- `sca-backup-*sql.gz`
- `sdp-backup-*sql.gz`
- `/usr/lib/sca/patterns/local` (necessário apenas se você criar padrões personalizados)

6. Ative novamente a aplicação SCA com:

```
scadb reset agents
```

PROCEDIMENTO 2.11 RESTAURANDO O BANCO DE DADOS

Para restaurar o banco de dados do backup, faça o seguinte:

1. Efetue login como usuário `root` no console do sistema do servidor que executa a aplicação SCA.
2. Copie os armazenamentos TAR `sca-backup-*sql.gz` e `sdp-backup-*sql.gz` mais recentes para o servidor da aplicação SCA.
3. Para descompactar os arquivos, execute:

```
gzip -d *-backup-*sql.gz
```

4. Para importar os dados para o banco de dados, execute:

```
scadb import sca-backup-*sql
```

5. Se você usa o banco de dados de criação de padrões para criar seus próprios padrões, importe também os seguintes dados com:

```
sdpdb import sdp-backup-*sql
```

6. Se você usa padrões personalizados, restaure também `/usr/lib/sca/patterns/local` dos dados do backup.
7. Ative novamente a aplicação SCA com:

```
scadb reset agents
```

8. Atualize os módulos de padrão no banco de dados com:

```
sdagent-patterns -u
```

2.4.3 Desenvolvendo padrões de análise personalizados

A aplicação SCA vem com um ambiente completo de desenvolvimento de padrões (o Banco de Dados de Padrões da SCA), que permite desenvolver padrões personalizados. Os padrões podem ser desenvolvidos em qualquer linguagem de programação. Para disponibilizá-los para o processo de análise do supportconfig, eles devem ser gravados em `/usr/lib/sca/patterns/local` e ser executáveis. Tanto a aplicação quanto a ferramenta SCA executam os padrões personalizados nos novos armazenamentos supportconfig como parte do relatório de análise. Para obter instruções detalhadas sobre como criar (e testar) seus próprios padrões, visite http://www.suse.com/communities/conversations/sca-pattern-development/.

2.5 Suporte aos módulos do Kernel

Um requisito importante para todo sistema operacional empresarial é o nível de suporte que você recebe do ambiente. Os módulos do Kernel são o conector mais relevante entre o hardware ("controladoras") e o sistema operacional. Cada módulo do Kernel no SUSE Linux Enterprise possui um flag `supported` (suportado) que pode ter três valores:

- "yes (sim)", portanto, `suportado`
- "externo", portanto, `suportado`
- "" (vazio, não definido) e `unsupported` (não suportado)

As seguintes regras são válidas:

- Por padrão, todos os módulos de um Kernel autorrecompilado são marcados como não suportados.
- Os módulos do Kernel suportados pelos parceiros do SUSE e distribuídos pelo `SUSE SolidDriver Program` são marcados como "externos".
- Se o flag `supported` não estiver definido, o carregamento do módulo contaminará o Kernel. Kernels contaminados não são suportados. Os módulos do Kernel não suportados estão incluídos em um pacote RPM adicional (`kernel-`*`TIPO`*`-extra`) e não são carregados

por padrão (*TIPO* = `default` | `xen` |...). Esses módulos não suportados também não estão disponíveis no instalador, e o pacote `kernel-`*TIPO*`-extra` não faz parte da mídia do SUSE Linux Enterprise.

- Os módulos do Kernel não incluídos em uma licença compatível com a licença do Kernel do Linux também contaminarão o Kernel. Para obter detalhes, consulte `/usr/src/linux/Documentation/sysctl/kernel.txt` e o estado de `/proc/sys/kernel/tainted`.

2.5.1 Informações técnicas

- Kernel do Linux: O valor de `/proc/sys/kernel/unsupported` usa o padrão `2` no SUSE Linux Enterprise 12 (`do not warn in syslog when loading unsupported modules`, não avisar no syslog ao carregar módulos não suportados). Esse padrão é usado no instalador e no sistema instalado. Consulte `/usr/src/linux/Documentation/sysctl/kernel.txt` para obter mais informações.

- **`modprobe`**: O utilitário **`modprobe`** de verificação de dependências de módulos e carregamento dos módulos apropriados confirma se o valor do flag é `supported` (suportado). Se o valor for “sim” ou “externo”, o módulo será carregado, do contrário, não. Para obter informações sobre como anular este comportamento, consulte a *Seção 2.5.2, “Trabalhando com módulos não suportados”*.

Nota

Em geral, o SUSE não suporta a remoção de módulos de armazenamento por **`modprobe -r`**.

2.5.2 Trabalhando com módulos não suportados

Embora a capacidade de suporte geral seja importante, algumas situações podem exigir o carregamento de um módulo não suportado (por exemplo, para fins de teste ou depuração, ou se o fornecedor de hardware disponibilizar um hotfix).

- Para anular o padrão, edite `/etc/modprobe.d/10-unsupported-modules.conf` e mude o valor da variável `allow_unsupported_modules` para `1`. Se for necessário um módulo não suportado no initrd, lembre-se de executar **`dracut -f`** para atualizar o initrd.

Para apenas tentar carregar um módulo uma vez, é possível usar a opção `--allow-unsupported-modules` com **`modprobe`**. Para obter mais informações, consulte a página de manual de **`modprobe`**.

- Durante a instalação, módulos não suportados podem ser adicionados por meio de discos de atualização de driver, e eles serão carregados. Para impor o carregamento de módulos não suportados durante a inicialização e posteriormente, use a opção de linha de comando do Kernel `oem-modules`. Durante a instalação e inicialização do pacote `suse-module-tools`, o flag do Kernel `TAINT_NO_SUPPORT` (`/proc/sys/kernel/tainted`) será avaliado. Se o Kernel já foi contaminado, `allow_unsupported_modules` será habilitado. Isso impede que módulos não suportados acessem o sistema que está sendo instalado. Se não houver nenhum módulo não suportado durante a instalação e não for usada a outra opção de linha de comando especial do Kernel (`oem-modules=1`), o padrão ainda será de não permitir módulos não suportados.

Lembre-se de que carregar e executar módulos não suportados tornam o Kernel e todo o sistema não suportados pelo SUSE.

2.6 Para obter mais informações

- **`man supportconfig`**: A página de manual de **`supportconfig`**.
- **`man supportconfig.conf`**: A página de manual do arquivo de configuração supportconfig.
- **`man scatool`**: A página de manual de **`scatool`**.
- **`man scadb`**: A página de manual de **`scadb`**.
- **`man setup-sca`**: A página de manual de **`setup-sca`**.
- https://mariadb.com/kb/en/: A documentação do MariaDB.
- http://www.suse.com/communities/conversations/sca-pattern-development/: Instruções sobre como criar (e testar) seus próprios padrões da SCA.
- http://www.suse.com/communities/conversations/basic-server-health-check-supportconfig/: Uma verificação da saúde básica do servidor com o supportconfig.

- https://www.novell.com/communities/coolsolutions/cool_tools/create-your-own-supportconfig-plugin/: Criar seu próprio plug-in Supportconfig.
- http://www.suse.com/communities/conversations/creating-a-central-supportconfig-repository/: Criar um repositório central do Supportconfig.

3 YaST em modo de texto

Esta seção destina-se principalmente a administradores e especialistas do sistema que não executam um servidor X em seus sistemas e dependem da ferramenta de instalação baseada em texto. Ela contém informações básicas sobre como iniciar e operar o YaST em modo de texto.

O YaST em modo de texto usa a biblioteca ncurses para fornecer uma interface pseudográfica do usuário fácil. A biblioteca ncurses está instalada por padrão. O tamanho mínimo suportado do emulador de terminal no qual executar o YaST é de 80 x 25 caracteres.

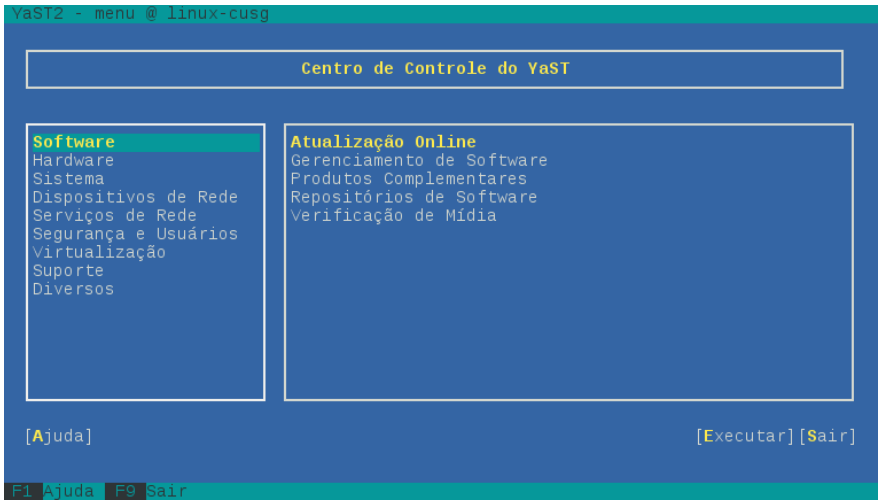


FIGURA 3.1 JANELA PRINCIPAL DO YAST EM MODO DE TEXTO

Quando você inicia o YaST em modo de texto, o centro de controle do YaST é exibido (consulte a *Figura 3.1*). A janela principal contém três áreas: O quadro esquerdo apresenta as categorias às quais pertencem os vários módulos. Esse frame torna-se ativo quando o YaST é iniciado e, portanto, é marcado por uma borda branca em negrito. A categoria ativa é realçada. O quadro direito apresenta uma visão geral dos módulos disponíveis na categoria ativa. O frame inferior contém os botões *Ajuda* e *Sair*.

Quando você inicia o centro de controle do YaST, a categoria *Software* é selecionada automaticamente. Use ↓ e ↑ para mudar a categoria. Para selecionar um módulo da categoria, ative o frame direito com → e, em seguida, use ↓ e ↑ para selecionar o módulo. Mantenha as teclas de seta pressionadas para rolar pela lista de módulos disponíveis. O módulo selecionado fica realçado. Pressione Enter para iniciar o módulo ativo.

Vários botões ou campos de seleção no módulo contêm uma letra realçada (amarelo por padrão). Use Alt–letra_realçada para selecionar um botão diretamente, em vez de navegar até ele com →|. Saia do centro de controle do YaST pressionando Alt–Q ou selecionando *Sair* e pressionando Enter.

Dica: Atualizando caixas de diálogo do YaST

Se uma caixa de diálogo do YaST for corrompida ou distorcida (por exemplo, ao redimensionar a janela), pressione Ctrl–L para atualizar e restaurar seu conteúdo.

3.1 Navegação em módulos

A seguinte descrição dos elementos de controle nos módulos do YaST pressupõe que todas as teclas de função e combinações de teclas Alt funcionam e que não estão atribuídas a funções globais diferentes. Leia a *Seção 3.2, "Restrição de combinações de tecla"* para obter informações sobre possíveis exceções.

Navegação entre botões e listas de seleção

Use →| para navegar entre os botões e frames contendo listas de seleção. Para navegar na ordem inversa, use combinações de Alt–→| ou Shift–→|.

Navegação em listas de seleção

Use as teclas de seta (↑ e ↓) para navegar entre os elementos individuais em um frame ativo que contenha uma lista de seleção. Se entradas individuais em um frame excederem a sua largura, use Shift–→ ou Shift–← para mover a barra de rolagem horizontalmente para a direita e esquerda. Alternativamente, use Ctrl–E ou Ctrl–A. Será possível também utilizar essa combinação se o uso de → ou ← resultar na mudança do frame ativo ou da lista de seleção atual, como no centro de controle.

Botões, botões de opção e caixas de seleção

Para selecionar botões com colchetes vazios (caixas de seleção) ou parênteses vazios (botões de opção), pressione Space ou Enter. Alternativamente, pode-se selecionar botões de opção e caixas de seleção diretamente com Alt–letra_realçada. Nesse caso, não é necessário confirmar com Enter. Se você navegar até um item com →|, pressione Enter para executar a ação selecionada ou ativar o item de menu respectivo.

Teclas de função

As teclas F (F1 a F12) permitem acesso rápido aos vários botões. As combinações de teclas de função disponíveis (Fx) são mostradas na linha inferior da tela do YaST. As teclas de função que são realmente mapeadas para cada botão dependem do módulo do YaST ativo, pois módulos diferentes oferecem botões diferentes (*Detalhes*, *Informações*, *Adicionar*, *Apagar*, etc.). Use F10 para *Aceitar*, *OK*, *Avançar* e *Concluir*. Pressione F1 para acessar a ajuda do YaST.

Usando a árvore de navegação no modo ncurses

Alguns módulos do YaST usam uma árvore de navegação na parte esquerda da janela para seleção de caixas de diálogo de configuração. Use as teclas de seta (↑ e ↓) para navegar na árvore. Use Space para abrir ou fechar itens da árvore. No modo ncurses, você deve pressionar Enter após uma seleção na árvore de navegação, a fim de mostrar a caixa de diálogo selecionada. Esse é um comportamento intencional que visa reduzir o tempo gasto para redesenhar durante a navegação na árvore.

Seleção de Software no Módulo Instalação de Software

Use os filtros à esquerda para limitar a quantidade de pacotes exibidos. Os pacotes instalados estão marcados com a letra i . Para mudar o status de um pacote, pressione Space ou Enter . Se preferir, use o menu *Ações* para selecionar a mudança de status necessária (instalar, apagar, atualizar, proibir ou bloquear).

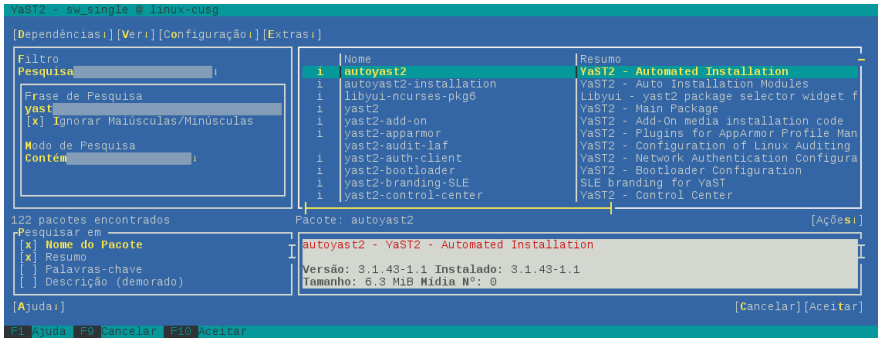


FIGURA 3.2 MÓDULO DE INSTALAÇÃO DE SOFTWARE

3.2 Restrição de combinações de tecla

Se o seu gerenciador de janelas usar combinações Alt globais, as combinações Alt no YaST talvez não funcionem. Teclas como Alt ou Shift também podem ser ocupadas pelas configurações do terminal.

Substituição de Alt por Esc

Os atalhos com Alt podem ser executados com Esc em vez de Alt. Por exemplo, Esc–H substitui Alt–H. (Primeiro pressione Esc, *depois* H.)

Navegação para trás e para frente com Ctrl–F e Ctrl–B

Se as combinações de Alt e Shift estiverem ocupadas pelo gerenciador de janelas ou pelo terminal, use as combinações Ctrl–F (para frente) e Ctrl–B (para trás).

Restrição de teclas de função

As teclas F também são usadas para funções. Certas teclas de função podem estar ocupadas pelo terminal e talvez não estejam disponíveis para o YaST. No entanto, as combinações de teclas Alt e teclas de função devem estar sempre disponíveis em um console de texto puro.

3.3 Opções de linha de comando do YaST

Além da interface de modo de texto, o YaST oferece uma interface de linha de comando pura. Para obter uma lista das opções de linha de comando do YaST, digite:

```
yast -h
```

3.3.1 Iniciando os módulos individuais

Para economizar tempo, os módulos do YaST individuais podem ser iniciados diretamente. Para iniciar um módulo, digite:

```
yast <module_name>
```

Exiba uma lista de todos os nomes de módulos disponíveis no seu sistema com **`yast -l`** ou **`yast --list`**. Inicie o módulo de rede, por exemplo, com **`yast lan`**.

3.3.2 Instalando pacotes a partir da linha de comando

Se você sabe o nome de um pacote e este é fornecido por qualquer um dos seus repositórios de instalação ativos, você pode usar a opção de linha de comando `-i` para instalar o pacote:

```
yast -i <package_name>
```

ou

```
yast --install <package_name>
```

`nome_do_pacote` pode ser um único nome de pacote abreviado, por exemplo `gvim`, instalado com verificação de dependência, ou o caminho completo para um pacote RPM, instalado sem verificação de dependência.

Se você precisar de um utilitário de gerenciamento de software baseado em linha de comando com funcionalidade adicional à fornecida pelo YaST, considere a possibilidade de usar o Zypper. Esse utilitário usa a mesma biblioteca de gerenciamento de software que também é a base do gerenciador de pacote do YaST. O uso básico do Zypper está apresentado na *Seção 7.1, “Usando o zypper”*.

3.3.3 Parâmetros de linha de comando dos módulos do YaST

Para usar a funcionalidade do YaST em scripts, ele oferece suporte a linha de comando para módulos individuais. Nem todos os módulos têm suporte para linha de comando. Para exibir as opções disponíveis de um módulo, digite:

```
yast <module_name> help
```

Se um módulo não fornecer suporte para linha de comando, ele será iniciado no modo de texto e a seguinte mensagem aparecerá:

```
This YaST module does not support the command line interface.
```

4 Recuperação de sistema e gerenciamento de instantâneos com o Snapper

Criar instantâneos do sistema de arquivos com a funcionalidade de fazer rollbacks no Linux era um recurso bastante solicitado no passado. O Snapper, em conjunto com o sistema de arquivos `Btrfs` ou os volumes LVM com aprovisionamento dinâmico, agora cumpre esse papel.

O `Btrfs`, um novo sistema de arquivos de gravação de cópia do Linux, suporta instantâneos de sistema de arquivos (uma cópia do estado de um subvolume em determinado ponto no tempo) de subvolumes (um ou mais sistemas de arquivos que podem ser montados separadamente em cada partição física). Os instantâneos também são suportados em volumes LVM com aprovisionamento dinâmico formatados com XFS, Ext4 ou Ext3. O Snapper permite criar e gerenciar esses instantâneos. Ele vem com uma linha de comando e uma interface do YaST. Desde o SUSE Linux Enterprise Server 12, também é possível inicializar de instantâneos `Btrfs`. Consulte a *Seção 4.3, "Rollback do sistema por inicialização de instantâneos"* para obter mais informações.

Usando o Snapper, é possível executar as seguintes tarefas:

- Desfazer mudanças no sistema feitas pelo **`zypper`** e pelo YaST. Consulte a *Seção 4.2, "Usando o Snapper para desfazer mudanças"* para obter os detalhes.
- Restaurar arquivos de instantâneos anteriores. Consulte a *Seção 4.2.2, "Usando o Snapper para restaurar arquivos"* para obter os detalhes.
- Fazer rollback do sistema inicializando de um instantâneo. Consulte a *Seção 4.3, "Rollback do sistema por inicialização de instantâneos"* para obter os detalhes.
- Criar manualmente instantâneos de forma simultânea e gerenciar instantâneos existentes. Consulte a *Seção 4.5, "Criando e gerenciando instantâneos manualmente"* para obter os detalhes.

4.1 Configuração padrão

O Snapper no SUSE Linux Enterprise Desktop foi configurado para atuar como uma “ferramenta para desfazer e recuperar” mudanças no sistema. Por padrão, a partição raiz (`/`) do SUSE Linux Enterprise Desktop está formatada com `Btrfs` . A captura de instantâneos será automaticamente habilitada se a partição raiz (`/`) for grande o suficiente (aproximadamente mais de 8 GB). A criação de instantâneos em partições diferentes de `/` não está habilitada por padrão.

Quando um instantâneo é criado, tanto o instantâneo quanto o original apontam para os mesmos blocos no sistema de arquivos. Por isso, o instantâneo inicialmente não ocupa espaço adicional no disco. Se os dados do sistema de arquivos original forem modificados, os blocos dos dados modificados serão copiados, enquanto os blocos dos dados antigos serão mantidos no instantâneo. Portanto, o instantâneo ocupa a mesma quantidade de espaço que os dados modificados. Ao longo do tempo, a quantidade de espaço alocada por um instantâneo cresce constantemente. Como consequência, a exclusão de arquivos do sistema de arquivos `Btrfs` que contém instantâneos pode *não* liberar espaço em disco!

Nota: Local do instantâneo

Os instantâneos residem sempre na mesma partição ou subvolume no qual foram criados. Não é possível armazenar os instantâneos em uma partição ou um subvolume diferente.

Como resultado, as partições com os instantâneos precisam ser maiores que as partições “normais”. A quantidade exata depende bastante do número de instantâneos mantidos e da quantidade de modificações de dados. De acordo com a prática, convém usar o dobro do tamanho que seria usado normalmente.

Embora os próprios instantâneos não se diferenciem no sentido técnico, nós os distinguimos em três tipos, com base na ocasião em foram criados:

TIPOS DE INSTANTÂNEOS

Instantâneos de Linha do Tempo

Um único instantâneo é criado a cada hora. Instantâneos antigos são apagados automaticamente. Por padrão, o primeiro instantâneo dos últimos dez dias, meses e anos são mantidos. Os instantâneos de linha do tempo estão habilitados por padrão, exceto para a partição raiz.

Instantâneos de Instalação

Sempre que um ou mais pacotes são instalados com o YaST ou o Zypper, um par de instantâneos é criado: um antes do início da instalação (“Pré”) e outro após o término da instalação (“Pós”). Se um componente importante do sistema, como o kernel, for instalado, o par de instantâneos será marcado como importante (`important=yes`). Instantâneos antigos são apagados automaticamente. Por padrão, os dez últimos instantâneos importantes e os dez últimos instantâneos “regulares” (incluindo os instantâneos de administração) são mantidos. Instantâneos de instalação são habilitados, por padrão.

Instantâneos de Administração

Sempre que você administra o sistema com o YaST, um par de instantâneos é criado: um quando algum módulo do YaST é iniciado (“Pré”) e outro quando o módulo é fechado (“Pós”). Instantâneos antigos são apagados automaticamente. Por padrão, os dez últimos instantâneos importantes e os dez últimos instantâneos “regulares” (incluindo os instantâneos de instalação) são mantidos. Instantâneos de administração são habilitados, por padrão.

Alguns diretórios precisam ser excluídos dos instantâneos por diversos motivos. A seguinte lista mostra todos os diretórios que são excluídos:

DIRETÓRIOS QUE SÃO EXCLUÍDOS DOS INSTANTÂNEOS

`/boot/grub2/x86_64-efi,`

O rollback da configuração do carregador de boot não é suportado.

`/home`

Se `/home` não residir em uma partição separada, ele será excluído para evitar perda de dados nos rollbacks.

`/opt`, `/var/opt`

Geralmente, produtos de terceiros e complementos são instalados em `/opt`. Ele é excluído para evitar a desinstalação dos aplicativos nos rollbacks.

`/srv`

Contém dados de servidores Web e FTP. Ele é excluído para evitar perda de dados nos rollbacks.

`/tmp`, `/var/tmp`, `/var/crash`

Todos os diretórios com arquivos temporários são excluídos dos instantâneos.

`/var/lib/named`

Contém dados da zona do servidor DNS. Excluído dos instantâneos para garantir que o servidor de nomes funcione após um rollback.

`/var/lib/mailman`, `/var/spool`

Diretórios com e-mails ou filas de e-mails são excluídos para evitar perda de e-mails após um rollback.

`/var/lib/pgqsl`

Contém dados do PostgreSQL.

`/var/log`

Localização do Arquivo de Registro. Excluído dos instantâneos para permitir a análise do arquivo de registro após o rollback de um sistema com defeito.

4.1.1 Personalizando a configuração

O SUSE Linux Enterprise Desktop vem com uma configuração padrão lógica, que deve ser suficiente na maioria dos casos de uso. No entanto, todos os aspectos da criação automática e da manutenção de instantâneos podem ser configurados de acordo com as suas necessidades.

4.1.1.1 Desabilitando/Habilitando instantâneos

Cada um dos três tipos de instantâneos (linha do tempo, instalação, administração) pode ser habilitado ou desabilitado de forma independente.

Desabilitando/Habilitando Instantâneos de Linha do Tempo

Habilitar. `snapper -c root set-config "TIMELINE_CREATE=yes"`

Desabilitar. `snapper -c root set-config "TIMELINE_CREATE=no"`

Os instantâneos de linha do tempo estão habilitados por padrão, exceto para a partição raiz.

Desabilitando/Habilitando Instantâneos de Instalação

Habilitar: Instale o pacote `snapper-zypp-plugin`

Desabilitar: Desinstale o pacote `snapper-zypp-plugin`

Instantâneos de instalação são habilitados, por padrão.

Desabilitando/Habilitando Instantâneos de Administração

Habilitar: Defina `USE_SNAPPER` como `yes` em `/etc/sysconfig/yast2`.

Desabilitar: Defina `USE_SNAPPER` como `no` em `/etc/sysconfig/yast2`. Instantâneos de administração são habilitados, por padrão.

4.1.1.2 Controlando instantâneos de instalação

A criação de pares de instantâneos ao instalar pacotes com o YaST ou o Zypper é administrada pelo `snapper-zypp-plugin`. O arquivo de configuração XML `/etc/snapper/zypp-plugin.conf` define quando criar instantâneos. Por padrão, o arquivo é parecido com o seguinte:

```
 1 <?xml version="1.0" encoding="utf-8"?>
 2 <snapper-zypp-plugin-conf>
 3  <solvables>
 4   <solvable match="w" ❶ important="true" ❷>kernel-* ❸</solvable>
 5   <solvable match="w" important="true">dracut</solvable>
 6   <solvable match="w" important="true">glibc</solvable>
 7   <solvable match="w" important="true">systemd*</solvable>
 8   <solvable match="w" important="true">udev</solvable>
 9   <solvable match="w">*</solvable> ❹
10  </solvables>
11 </snapper-zypp-plugin-conf>
```

❶ O atributo de correspondência define se o padrão é um curinga no estilo shell do Unix (`w`) ou uma expressão regular Python (`re`).

❷ Se houver correspondência do padrão especificado e o pacote correspondente estiver marcado como importante (por exemplo, pacotes do Kernel), o instantâneo também será marcado como importante.

❸ Padrão de correspondência com o nome de um pacote. Com base na configuração do atributo `match`, caracteres especiais são interpretados como curingas do shell ou expressões regulares. Este padrão corresponde todos os nomes de pacotes que começam com `kernel-`.

❹ Esta linha corresponde todos os pacotes incondicionalmente.

Com este instantâneo de configuração, os pares são criados sempre que um pacote é instalado (linha 9). Quando são instalados pacotes do Kernel, dracut, glibc, systemd ou udev marcados como importantes, o par de instantâneos também é marcado como importante (linhas 4 a 8). Todas as regras são avaliadas.

Para desabilitar uma regra, apague-a ou desative-a usando comentários XML. Para impedir que o sistema crie pares de instantâneos para cada pacote de instalação, por exemplo, comente na linha 9:

```
 1 <?xml version="1.0" encoding="utf-8"?>
 2 <snapper-zypp-plugin-conf>
 3  <solvables>
 4   <solvable match="w" important="true">kernel-*</solvable>
 5   <solvable match="w" important="true">dracut</solvable>
 6   <solvable match="w" important="true">glibc</solvable>
 7   <solvable match="w" important="true">systemd*</solvable>
 8   <solvable match="w" important="true">udev</solvable>
 9   <!-- <solvable match="w">*</solvable> -->
10  </solvables>
11 </snapper-zypp-plugin-conf>
```

4.1.1.3 Controlando o armazenamento de instantâneos

Instantâneos ocupam espaço no disco. Para evitar que os discos fiquem sem espaço e, por essa razão, provoquem interrupções de sistema, os instantâneos antigos são apagados automaticamente. Por padrão, os seguintes instantâneos são mantidos:

- o primeiro instantâneo dos últimos dez dias, meses e anos
- os últimos dez pares de instantâneos de instalação marcados como importantes
- os últimos dez instantâneos de instalação/administração

Consulte a *Seção 4.4.1, "Gerenciando configurações existentes"* para ver instruções sobre como mudar os valores.

4.1.1.4 Usando o Snapper em volumes LVM com aprovisionamento dinâmico

Além dos instantâneos nos sistemas de arquivos `Btrfs`, o Snapper também suporta criação de instantâneos em volumes LVM com aprovisionamento dinâmico (instantâneos em volumes LVM regulares *não* são suportados) formatados com XFS, Ext4 ou Ext3. Para obter mais informações e instruções de configuração de volumes LVM, consulte a *Book "*Deployment Guide*" 12 "Advanced Disk Setup"12.2 "LVM Configuration"*.

Para usar o Snapper em um volume LVM com aprovisionamento dinâmico, crie para ele uma configuração do Snapper. No LVM, é necessário especificar o sistema de arquivos com `--fstype=lvm(`*`SISTEMADEARQUIVOS`*`)`. `ext3`, `etx4` ou `xfs` são valores válidos para *`SISTEMADEARQUIVOS`*. Exemplo:

```
snapper -c lvm create-config --fstype="lvm(xfs)" /thin_lvm
```

É possível ajustar essa configuração de acordo com as suas necessidades conforme descrito na *Seção 4.4.1, "Gerenciando configurações existentes"*.

4.2 Usando o Snapper para desfazer mudanças

O Snapper no SUSE Linux Enterprise Desktop é pré-configurado para atuar como uma ferramenta capaz de desfazer as mudanças feitas pelo **`zypper`** e pelo YaST. Para esta finalidade, o Snapper é configurado para criar um par de instantâneos antes e depois de cada execução do **`zypper`** e do YaST. O Snapper permite também restaurar arquivos do sistema que foram acidentalmente apagados ou modificados. Os instantâneos de linha do tempo da partição raiz precisam ser habilitados para essa finalidade. Consulte a *Seção 4.1.1.1, "Desabilitando/Habilitando instantâneos"* para obter detalhes.

Por padrão, os instantâneos automáticos, conforme descrito anteriormente, são configurados para a partição raiz e seus subvolumes. Para disponibilizar os instantâneos para outras partições, como `/home`, é possível criar configurações personalizadas.

Importante: Desfazendo mudanças X rollback

Ao trabalhar com instantâneos para restaurar dados, é importante saber que há dois cenários fundamentalmente distintos nos quais o Snapper pode atuar:

Desfazendo mudanças

Ao desfazer mudanças conforme descrito a seguir, dois instantâneos são comparados, e as mudanças entre eles são desfeitas. O uso deste método também permite selecionar explicitamente os arquivos que devem ser restaurados.

Rollback

Ao fazer rollbacks conforme descrito na *Seção 4.3, "Rollback do sistema por inicialização de instantâneos"*, o sistema é redefinido para o estado do momento em que o instantâneo foi criado.

Ao desfazer mudanças, é possível também comparar um instantâneo com o sistema atual. Ao restaurar *todos* os arquivos com base nesta comparação, o resultado será igual a fazer rollback. No entanto, o uso do método descrito na *Seção 4.3, "Rollback do sistema por inicialização de instantâneos"* para rollbacks deve ser preferencial, pois é mais rápido e permite revisar o sistema antes de fazer rollback.

Atenção: Consistência de dados

Não existe nenhum mecanismo que assegure a consistência dos dados ao criar um instantâneo. Sempre que um arquivo (por exemplo, um banco de dados) for gravado enquanto o instantâneo estiver sendo criado, o resultado será um arquivo com defeito ou parcialmente gravado. A restauração desse arquivo causa problemas. Além disso, alguns arquivos do sistema, como `/etc/mtab`, nunca devem ser restaurados. Portanto, é altamente recomendável *sempre* revisar com cuidado a lista de arquivos modificados e suas diffs. Restaure apenas arquivos realmente relevantes à ação que deseja reverter.

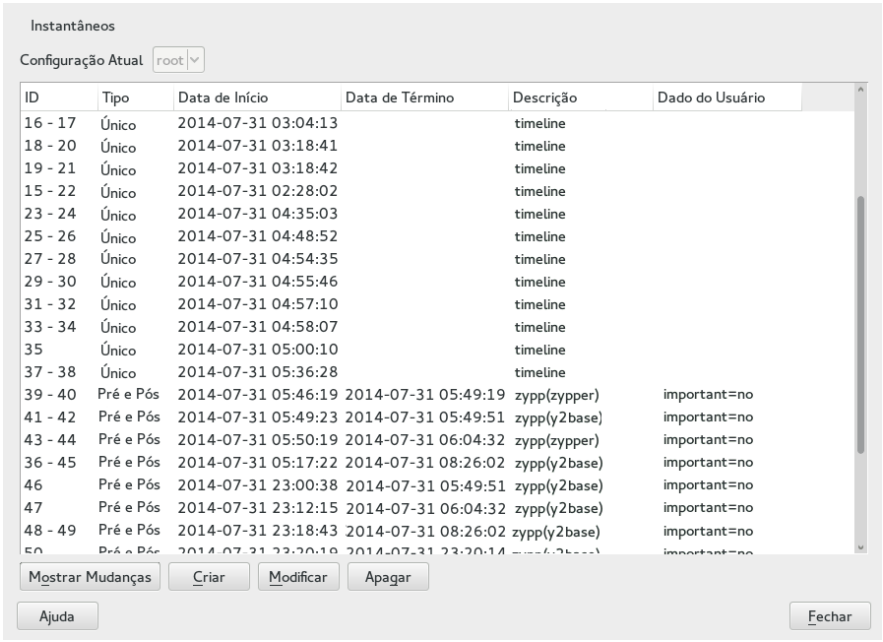
4.2.1 Desfazendo mudanças do YaST e Zypper

Se você configurar a partição raiz com o `Btrfs` durante a instalação, o Snapper, pré-configurado para fazer rollbacks das mudanças do YaST ou do Zypper, será instalado automaticamente. Sempre que você iniciar um módulo do YaST ou uma transação do Zypper, serão criados dois instantâneos: um "pré-instantâneo", que captura o estado do sistema de arquivos antes do início do módulo, e um "pós-instantâneo" após o término do módulo.

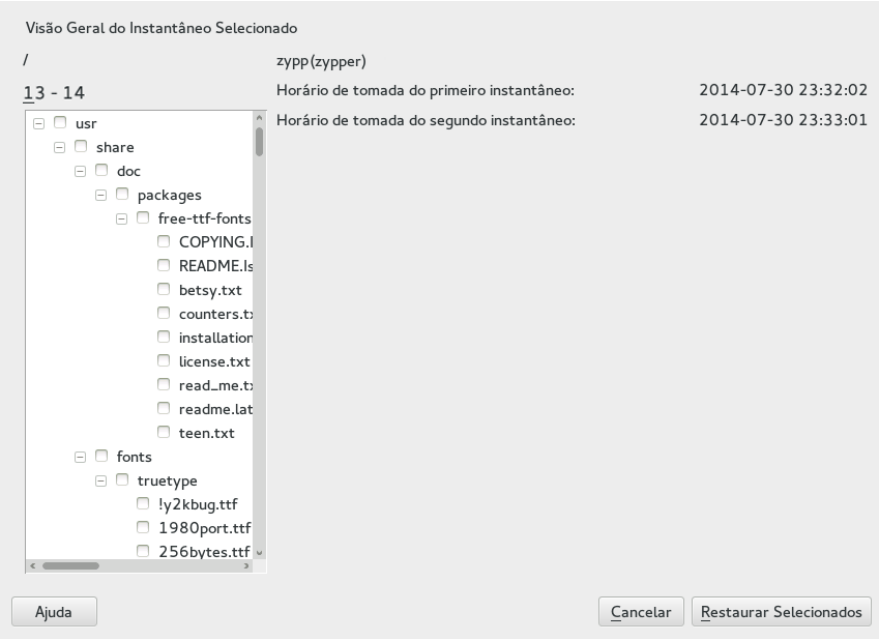
Usando o módulo Snapper do YaST ou a ferramenta de linha de comando **`snapper`**, é possível desfazer as mudanças feitas pelo YaST/Zypper restaurando os arquivos do "pré-instantâneo". Pela comparação dos dois instantâneos, as ferramentas permitem ver quais arquivos foram modificados. É possível também exibir as diferenças entre as duas versões de um arquivo (diff).

PROCEDIMENTO 4.1 DESFAZENDO MUDANÇAS USANDO O MÓDULO *SNAPPER* DO YAST

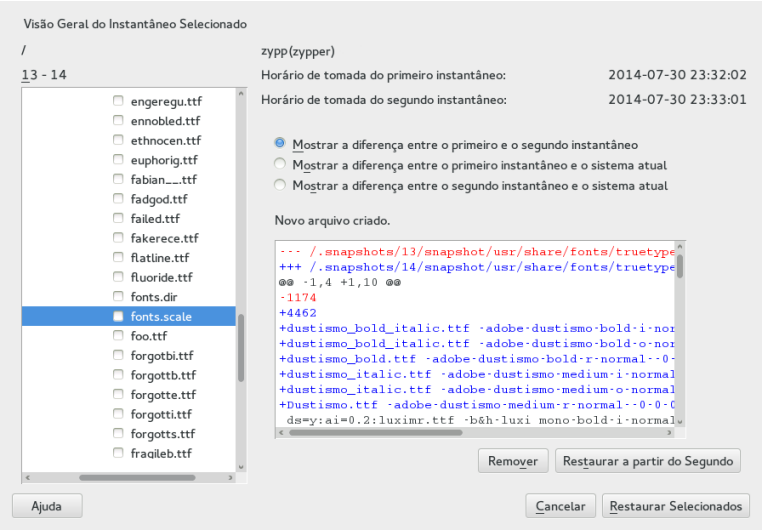
1. Inicie o módulo *Snapper* pela seção *Diversos* no YaST ou digitando **`yast2 snapper`**.
2. Confirme se a *Configuração Atual* está definida como *root*. Esse é sempre o caso, a não ser que você tenha adicionado manualmente configurações personalizadas do Snapper.
3. Escolha o par de pré e pós-instantâneos na lista. Ambos os pares de instantâneos do YaST e do Zypper são do tipo *Pré e Pós*. Os instantâneos do YaST são denominados `zypp(y2base)` na *coluna Descrição*; os instantâneos do Zypper são denominados `zypp(zypper)`.


Instantâneos
Configuração Atual
root
ID
Tipo
Data de Início
Data de Término
Descrição
Dado do Usuário
16 - 17 Único 2014-07-31 03:04:13 timeline
18 - 20 Único 2014-07-31 03:18:41 timeline
19 - 21 Único 2014-07-31 03:18:42 timeline
15 - 22 Único 2014-07-31 02:28:02 timeline
23 - 24 Único 2014-07-31 04:35:03 timeline
25 - 26 Único 2014-07-31 04:48:52 timeline
27 - 28 Único 2014-07-31 04:54:35 timeline
29 - 30 Único 2014-07-31 04:55:46 timeline
31 - 32 Único 2014-07-31 04:57:10 timeline
33 - 34 Único 2014-07-31 04:58:07 timeline
35 Único 2014-07-31 05:00:10 timeline
37 - 38 Único 2014-07-31 05:36:28 timeline
39 - 40 Pré e Pós 2014-07-31 05:46:19 2014-07-31 05:49:19 zypp(zypper) important=no
41 - 42 Pré e Pós 2014-07-31 05:49:23 2014-07-31 05:49:51 zypp(y2base) important=no
43 - 44 Pré e Pós 2014-07-31 05:50:19 2014-07-31 06:04:32 zypp(zypper) important=no
36 - 45 Pré e Pós 2014-07-31 05:17:22 2014-07-31 08:26:02 zypp(y2base) important=no
46 Pré e Pós 2014-07-31 23:00:38 2014-07-31 05:49:51 zypp(y2base) important=no
47 Pré e Pós 2014-07-31 23:12:15 2014-07-31 06:04:32 zypp(y2base) important=no
48 - 49 Pré e Pós 2014-07-31 23:18:43 2014-07-31 08:26:02 zypp(y2base) important=no
Mostrar Mudanças
Criar
Modificar
Apagar
Ajuda
Fechar

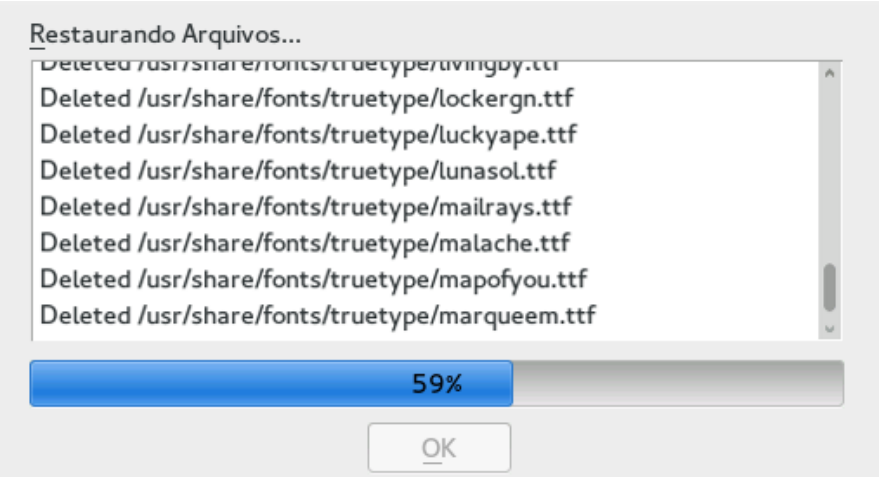
4. Clique em *Mostrar Mudanças* para abrir a lista de arquivos que são diferentes entre os dois instantâneos.



5. Revise a lista de arquivos. Para exibir a diferença (“diff”) entre a versão pré e pós de um arquivo, selecione-o na lista.



6. Para restaurar um ou mais arquivos, selecione os arquivos ou diretórios relevantes marcando a respectiva caixa de seleção. Clique em *Restaurar Selecionados* e clique em *Sim* para confirmar a ação.



Para restaurar um único arquivo, ative sua tela de comparação clicando em seu nome. Clique em *Restaurar a partir do Primeiro* e clique em *Sim* para confirmar sua seleção.

PROCEDIMENTO 4.2 DESFAZENDO MUDANÇAS USANDO O COMANDO `snapper`

1. Obtenha uma lista dos instantâneos do YaST e do Zypper executando o comando **`snapper list -t pre-post`**. Os instantâneos do YaST são denominados `yast` *`nome_do_módulo`* na *coluna Descrição*; os instantâneos do Zypper são denominados `zypp(zypper)`.

```
root # snapper list -t pre-post
Pre # | Post # | Pre Date                          | Post Date                         | Description
------+--------+-----------------------------------+-----------------------------------+--------------
311   | 312    | Tue 06 May 2014 14:05:46 CEST | Tue 06 May 2014 14:05:52 CEST | zypp(y2base)
340   | 341    | Wed 07 May 2014 16:15:10 CEST | Wed 07 May 2014 16:15:16 CEST | zypp(zypper)
342   | 343    | Wed 07 May 2014 16:20:38 CEST | Wed 07 May 2014 16:20:42 CEST | zypp(y2base)
344   | 345    | Wed 07 May 2014 16:21:23 CEST | Wed 07 May 2014 16:21:24 CEST | zypp(zypper)
346   | 347    | Wed 07 May 2014 16:41:06 CEST | Wed 07 May 2014 16:41:10 CEST | zypp(y2base)
348   | 349    | Wed 07 May 2014 16:44:50 CEST | Wed 07 May 2014 16:44:53 CEST | zypp(y2base)
350   | 351    | Wed 07 May 2014 16:46:27 CEST | Wed 07 May 2014 16:46:38 CEST | zypp(y2base)
```

2. Obtenha uma lista dos arquivos modificados de um par de instantâneos com **snapper status** *PRÉ..PÓS*. Os arquivos com mudanças de conteúdo são marcados com *c*, os arquivos que foram adicionados são marcados com + e os arquivos apagados são marcados com -.

```
root # snapper status 350..351
+..... /usr/share/doc/packages/mikachan-fonts
+..... /usr/share/doc/packages/mikachan-fonts/COPYING
+..... /usr/share/doc/packages/mikachan-fonts/dl.html
c..... /usr/share/fonts/truetype/fonts.dir
c..... /usr/share/fonts/truetype/fonts.scale
+..... /usr/share/fonts/truetype/#####-p.ttf
+..... /usr/share/fonts/truetype/#####-pb.ttf
+..... /usr/share/fonts/truetype/#####-ps.ttf
+..... /usr/share/fonts/truetype/#####.ttf
c..... /var/cache/fontconfig/7ef2298fde41cc6eeb7af42e48b7d293-x86_64.cache-4
c..... /var/lib/rpm/Basenames
c..... /var/lib/rpm/Dirnames
c..... /var/lib/rpm/Group
c..... /var/lib/rpm/Installtid
c..... /var/lib/rpm/Name
c..... /var/lib/rpm/Packages
c..... /var/lib/rpm/Providename
c..... /var/lib/rpm/Requirename
c..... /var/lib/rpm/Sha1header
c..... /var/lib/rpm/Sigmd5
```

3. Para exibir a diff de determinado arquivo, execute **snapper diff** *PRÉ..PÓS NOMEDOARQUIVO*. Se você não especificar *NOMEDOARQUIVO*, será exibida a diff de todos os arquivos.

```
root # snapper diff 350..351 /usr/share/fonts/truetype/fonts.scale
--- /.snapshots/350/snapshot/usr/share/fonts/truetype/fonts.scale 2014-04-23
 15:58:57.000000000 +0200
+++ /.snapshots/351/snapshot/usr/share/fonts/truetype/fonts.scale 2014-05-07
 16:46:31.000000000 +0200
```

```
@@ -1,4 +1,4 @@
-1174
+1486
 ds=y:ai=0.2:luximr.ttf -b&h-luxi mono-bold-i-normal--0-0-0-0-c-0-iso10646-1
 ds=y:ai=0.2:luximr.ttf -b&h-luxi mono-bold-i-normal--0-0-0-0-c-0-iso8859-1
[...]
```

4. Para restaurar um ou mais arquivos, execute **snapper -v undochange** *PRÉ..PÓS NOMESDOSARQUIVOS*. Se você não especificar os *NOMESDOSARQUIVOS*, todos os arquivos serão restaurados.

```
root # snapper -v undochange 350..351
     create:0 modify:13 delete:7
     undoing change...
     deleting /usr/share/doc/packages/mikachan-fonts
     deleting /usr/share/doc/packages/mikachan-fonts/COPYING
     deleting /usr/share/doc/packages/mikachan-fonts/dl.html
     deleting /usr/share/fonts/truetype/#####-p.ttf
     deleting /usr/share/fonts/truetype/#####-pb.ttf
     deleting /usr/share/fonts/truetype/#####-ps.ttf
     deleting /usr/share/fonts/truetype/#####.ttf
     modifying /usr/share/fonts/truetype/fonts.dir
     modifying /usr/share/fonts/truetype/fonts.scale
     modifying /var/cache/fontconfig/7ef2298fde41cc6eeb7af42e48b7d293-
x86_64.cache-4
     modifying /var/lib/rpm/Basenames
     modifying /var/lib/rpm/Dirnames
     modifying /var/lib/rpm/Group
     modifying /var/lib/rpm/Installtid
     modifying /var/lib/rpm/Name
     modifying /var/lib/rpm/Packages
     modifying /var/lib/rpm/Providename
     modifying /var/lib/rpm/Requirename
     modifying /var/lib/rpm/Sha1header
     modifying /var/lib/rpm/Sigmd5
     undoing change done
```

Atenção: Revertendo adições de usuário

Não é recomendado reverter adições de usuário desfazendo mudanças com o Snapper. Como alguns diretórios são excluídos dos instantâneos, os arquivos pertencentes a estes usuários permanecerão no sistema de arquivos. Se for criado um usuário com o mesmo ID de usuário daquele que foi apagado, ele herdará os arquivos. Portanto, é altamente recomendável usar a ferramenta *Gerenciamento de Usuários e Grupos* do YaST para remover usuários.

4.2.2 Usando o Snapper para restaurar arquivos

Além dos instantâneos de instalação e administração, o Snapper cria instantâneos de linha do tempo. É possível usar os instantâneos de backup para restaurar arquivos que foram apagados acidentalmente ou para restaurar a versão anterior de um arquivo. Usando o recurso diff do Snapper, é possível também descobrir quais modificações foram feitas em determinado momento.

A capacidade de restaurar arquivos é interessante principalmente no que diz respeito a dados, que podem residir em subvolumes ou partições dos quais os instantâneos não são criados por padrão. Para restaurar arquivos de diretórios pessoais, por exemplo, crie uma configuração separada do Snapper para `/home` para criar instantâneos de linha do tempo automáticos. Consulte a *Seção 4.4, "Criando e modificando as configurações do Snapper"* para obter instruções.

Atenção: Restauração de arquivos X rollback

Os instantâneos criados do sistema de arquivos raiz (definido pela configuração raiz do Snapper) podem ser usados para fazer rollback do sistema. A forma recomendada de fazer o rollback é inicializar do instantâneo e depois fazer o rollback. Consulte a *Seção 4.3, "Rollback do sistema por inicialização de instantâneos"* para obter os detalhes.

É possível também fazer rollback restaurando todos os arquivos de um instantâneo do sistema de arquivos raiz, conforme descrito a seguir. No entanto, isso não é recomendado. É possível restaurar arquivos únicos, por exemplo, um arquivo de configuração do diretório `/etc`, mas não a lista completa de arquivos do instantâneo.

Esta restrição afeta apenas os instantâneos criados do sistema de arquivos raiz!

PROCEDIMENTO 4.3 RESTAURANDO ARQUIVOS USANDO O MÓDULO *SNAPPER* DO YAST

1. Inicie o módulo *Snapper* pela seção *Diversos* no YaST ou digitando **`yast2 snapper`**.
2. Selecione a *Configuração Atual* da qual escolher o instantâneo.
3. Selecione o instantâneo de linha do tempo do qual restaurar o arquivo e escolha *Mostrar Mudanças*. Os instantâneos de linha do tempo são do tipo *Único*, com um valor descritivo de *linha do tempo*.
4. Selecione um arquivo na caixa de texto clicando no nome dele. A diferença entre a versão do instantâneo e o sistema atual é exibida. Marque a caixa de seleção para escolher o arquivo para restauração. Faça isso para todos os arquivos que deseja restaurar.
5. Clique em *Restaurar Selecionados* e clique em *Sim* para confirmar a ação.

PROCEDIMENTO 4.4 RESTAURANDO ARQUIVOS USANDO O COMANDO `snapper`

1. Obtenha a lista de instantâneos de linha do tempo para determinada configuração executando o seguinte comando:

   ```
   snapper -c CONFIG list -t single | grep timeline
   ```

   `CONFIG` precisa ser substituído pela configuração existente do Snapper. Use **`snapper list-configs`** para exibir uma lista.
2. Obtenha a lista de arquivos modificados de determinado instantâneo executando o seguinte comando:

   ```
   snapper -c CONFIG status SNAPSHOT_ID>..0
   ```

   Substitua *`ID_DO_INSTANTÂNEO`* pelo ID do instantâneo do qual deseja restaurar o(s) arquivo(s).
3. Se preferir, liste as diferenças entre a versão do arquivo atual e a versão do instantâneo executando

   ```
   snapper -c CONFIG diff SNAPSHOT_ID..0 FILE NAME
   ```

   Se você não especificar *`<NOME DE ARQUIVO>`*, será mostrada a diferença de todos os arquivos.
4. Para restaurar um ou mais arquivos, execute

   ```
   snapper -c CONFIG -v undochange
   ```

```
SNAPSHOT_ID..0 FILENAME1 FILENAME2
```

Se você não especificar nomes de arquivos, todos os arquivos mudados serão restaurados.

4.3 Rollback do sistema por inicialização de instantâneos

A versão GRUB 2 incluída no SUSE Linux Enterprise Desktop é capaz de inicializar de instantâneos Btrfs. Juntamente com o recurso de rollback do Snapper, ela permite recuperar um sistema mal configurado. Todos os instantâneos criados pelo Snapper estão disponíveis para inicialização e podem ser selecionados no menu de boot.

Importante: Instantâneos inicializáveis

Apenas os instantâneos do sistema de arquivos raiz (definido na configuração raiz do Snapper) são inicializáveis.

Ao inicializar um instantâneo, as partes do sistema de arquivos incluídas no instantâneo são montadas como apenas leitura; todos os outros sistemas de arquivos e partes excluídos dos instantâneos são montados como leitura-gravação e podem ser modificados.

Importante: Desfazendo mudanças X rollback

Ao trabalhar com instantâneos para restaurar dados, é importante saber que há dois cenários fundamentalmente distintos nos quais o Snapper pode atuar:

Desfazendo mudanças

Ao desfazer mudanças conforme descrito na *Seção 4.2, "Usando o Snapper para desfazer mudanças"*, dois instantâneos são comparados e as mudanças entre eles são revertidas. O uso deste método também permite excluir explicitamente os arquivos selecionados para não serem restaurados.

Rollback

Ao fazer rollbacks conforme descrito a seguir, o sistema é redefinido para o estado do momento em que o instantâneo foi criado.

Para fazer rollback de um instantâneo inicializável, os seguintes requisitos devem ser atendidos. Em uma instalação padrão, o sistema é configurado apropriadamente.

REQUISITOS PARA ROLLBACK DE UM INSTANTÂNEO INICIALIZÁVEL

- O sistema de arquivos raiz precisa ser o Btrfs. A inicialização de instantâneos de volume LVM não é suportada.
- O sistema de arquivos raiz precisa estar em um único dispositivo, uma única partição e um único subvolume. Os diretórios excluídos dos instantâneos, como `/srv` (consulte *Diretórios que são excluídos dos instantâneos* para ver a lista completa) podem residir em partições separadas.
- O sistema precisa ser inicializável pelo carregador de boot instalado.

Para fazer rollback de um instantâneo inicializável, faça o seguinte:

1. Inicialize o sistema. No menu de boot, escolha *Bootable snapshots* (Instantâneos inicializáveis) e selecione o instantâneo que deseja inicializar. A lista de instantâneos é classificada por data: o instantâneo mais recente é listado primeiro.
2. Efetue login no sistema. Verifique com atenção se tudo funciona conforme esperado. Observe que você não poderá gravar em nenhum diretório que faça parte do instantâneo. Os dados gravados em outros diretórios *não* serão perdidos, independentemente do que você faça a seguir.
3. Dependendo se você deseja ou não fazer rollback, escolha a próxima etapa:
   a. Se o sistema estiver em um estado no qual você não deseja fazer rollback, reinicialize para inicializar no estado atual do sistema, escolher um instantâneo diferente ou iniciar o sistema de recuperação.
   b. Para fazer o rollback, execute

      ```
      sudo snapper rollback
      ```

      e reinicialize na sequência. Na tela de boot, escolha a entrada de boot padrão para reinicializar no sistema restaurado.

4.3.1 Limitações

O rollback do sistema *completo*, restauração do sistema completo exatamente para o mesmo estado em que estava quando o instantâneo foi criado, não é possível.

4.3.1.1 Diretórios excluídos dos instantâneos

Os instantâneos do sistema de arquivos raiz não contêm todos os diretórios. Consulte *Diretórios que são excluídos dos instantâneos* para ver os detalhes e motivos. Como consequência geral, os dados desses diretórios não são restaurados, resultando nas seguintes limitações.

Complementos e software de terceiros podem se tornar inutilizáveis após o rollback

Os aplicativos e complementos que instalam dados em subvolumes excluídos do instantâneo, como `/opt`, poderão não funcionar após o rollback, se outras partes dos dados dos aplicativos também forem instaladas em subvolumes incluídos no instantâneo. Reinstale o aplicativo ou complemento para resolver o problema.

Problemas de Acesso a Arquivos

Se um aplicativo mudar as permissões e/ou a propriedade do arquivo no meio tempo entre o instantâneo e o sistema atual, o aplicativo talvez não consiga acessar o arquivo. Redefina as permissões e/ou a propriedade dos arquivos afetados após o rollback.

Formatos de Dados Incompatíveis

Se um serviço ou aplicativo estabelecer um novo formato de dados no meio tempo entre o instantâneo e o sistema atual, o aplicativo talvez não consiga ler os arquivos de dados afetados após o rollback.

Subvolumes com Mistura de Códigos e Dados

Subvolumes como `/srv` podem incluir uma mistura de códigos e dados. O rollback pode resultar em código não funcional. A instalação de uma versão PHP menos eficiente, por exemplo, pode resultar em scripts PHP com defeito no servidor Web.

Dados do Usuário

Se o rollback remover usuários do sistema, os dados de propriedade desses usuários nos diretórios excluídos do instantâneo serão removidos. Se for criado um usuário com o mesmo ID de usuário, ele herdará os arquivos. Use uma ferramenta como **`find`** para localizar e remover arquivos órfãos.

4.3.1.2 Nenhum rollback dos dados do carregador de boot

Não é possível fazer rollback do carregador de boot, pois todas as "fases" do carregador de boot devem se ajustar. Isso não é garantido no caso de rollbacks.

4.4 Criando e modificando as configurações do Snapper

O modo como o Snapper se comporta é definido em um arquivo de configuração específico a cada partição ou subvolume `Btrfs`. Estes arquivos de configuração residem em `/etc/snapper/configs/`. A configuração padrão instalada com o Snapper para o diretório `/` é denominada `root`. Ela cria e gerencia os instantâneos do YaST e do Zypper, além do instantâneo de backup por hora do `/`.

É possível criar suas próprias configurações para outras partições formatadas com `Btrfs` ou subvolumes existentes em uma partição `Btrfs`. No exemplo a seguir, nós definimos uma configuração do Snapper para backup dos dados do servidor Web que residem em uma partição separada formatada por `Btrfs` montada em `/srv/www`.

Após a criação de uma configuração, é possível usar o próprio **`snapper`** ou o módulo *Snapper* do YaST para restaurar arquivos desses instantâneos. No YaST, você precisa selecionar a *Configuração Atual* e especificar a configuração do **`snapper`** com o switch global `-c` (por exemplo, **`snapper`** `-c myconfig` **`list`**).

Para criar uma nova configuração do Snapper, execute **`snapper create-config`**:

```
snapper -c www-data❶ create-config /srv/www❷
```

❶ Nome do arquivo de configuração.

❷ Ponto de montagem da partição ou subvolume `Btrfs` no qual criar instantâneos.

Este comando cria um novo arquivo de configuração `/etc/snapper/configs/www-data` com valores padrão lógicos (obtidos de `/etc/snapper/config-templates/default`). Consulte a *Seção 4.4.1, "Gerenciando configurações existentes"* para obter instruções de como ajustar os padrões.

Dica: Padrões de configuração

Os valores padrão para uma nova configuração são obtidos de `/etc/snapper/config-templates/default`. Para usar seu próprio conjunto de padrões, crie uma cópia desse arquivo no mesmo diretório e ajuste-o de acordo com as suas necessidades. Para usá-lo, especifique a opção `-t` com o comando create-config:

```
snapper -c www-data create-config -t my_defaults /srv/www
```

4.4.1 Gerenciando configurações existentes

O **`snapper`** oferece vários subcomandos para gerenciar configurações existentes. É possível listar, mostrar, apagar e modificá-las:

Listar Configurações

Use o comando **`snapper list-configs`** para obter todas as configurações existentes:

```
root # snapper list-configs
Config | Subvolume
-------+----------
root   | /
usr    | /usr
local  | /local
```

Apagar uma Configuração

Use o subcomando **`snapper`** `-c` *`CONFIG`* **`delete-config`** para apagar uma configuração. *`Config`* deve ser substituído pelo nome da configuração mostrado pelo **`snapper list-configs`**.

Mostrar uma Configuração

Use o subcomando **`snapper`** `-c` *`CONFIG`* **`get-config`** para exibir a configuração especificada. *`Config`* deve ser substituído pelo nome da configuração mostrado pelo **`snapper list-configs`**. Consulte a *Seção 4.4.1.1, "Dados de configuração"* para obter mais informações sobre opções de configuração.

Use o subcomando **`snapper -c CONFIG set-config OPÇÃO=VALOR`** para modificar uma opção na configuração especificada. *`Config`* deve ser substituído pelo nome da configuração mostrado pelo **`snapper list-configs`**. Os valores possíveis para *`OPÇÃO`* e *`VALOR`* estão listados na *Seção 4.4.1.1, "Dados de configuração"*.

4.4.1.1 Dados de configuração

Cada configuração possui uma lista das opções que podem ser modificadas por linha de comando. A seguinte lista mostra os detalhes de cada opção:

`ALLOW_GROUPS`, `ALLOW_USERS`

Conceder permissões para usar instantâneos a usuários regulares. Consulte a *Seção 4.4.1.2, "Usando o Snapper como usuário comum"* para obter mais informações.

O valor padrão é `""`.

`BACKGROUND_COMPARISON`

Define se os instantâneos pré e pós devem ser comparados em segundo plano após a criação.

O valor padrão é `"yes"` (sim).

EMPTY_PRE_POST_CLEANUP

Se definido como `yes` (sim), os pares de instantâneos pré e pós que forem iguais serão apagados.

O valor padrão é `"no"` (não).

EMPTY_PRE_POST_MIN_AGE

Define a duração mínima, em segundos, do par de instantâneos pré e pós iguais antes de ser automaticamente apagado.

O valor padrão é `"1800"`.

`FSTYPE`

Tipo de sistema de arquivos da partição. Não alterar.

O valor padrão é `"btrfs"`.

`NUMBER_CLEANUP`

Define se é para apagar automaticamente os pares de instantâneos de instalação e administração antigos quando o total de instantâneos exceder o número especificado com `NUMBER_LIMIT` *e* a duração especificada com `NUMBER_MIN_AGE`. Valores válidos: `yes`, `no`

O valor padrão é `"no"`.

Nota: Limite e duração

`NUMBER_LIMIT`, `NUMBER_LIMIT_IMPORTANT` e `NUMBER_MIN_AGE` são sempre avaliados. Os instantâneos são apagados apenas quando ocorrem *todas* as condições. Para sempre manter determinado número de instantâneos independentemente de sua duração, defina `NUMBER_MIN_AGE` como `0`. Por outro lado, para não manter os instantâneos após certa duração, defina `NUMBER_LIMIT` e `NUMBER_LIMIT_IMPORTANT` como `0`.

`NUMBER_LIMIT`

Define quantos pares de instantâneos de instalação e administração não marcados como importantes manter se `NUMBER_CLEANUP` estiver definido como `yes`. Apenas os instantâneos mais recentes são mantidos.

O valor padrão é `"50"`.

`NUMBER_LIMIT_IMPORTANT`

Define quantos pares de instantâneos marcados como importantes manter se `NUMBER_CLEANUP` estiver definido como `yes`. Apenas os instantâneos mais recentes são mantidos.

O valor padrão é `"10"`.

`NUMBER_MIN_AGE`

Define a duração mínima, em segundos, do par de instantâneos antes de ser automaticamente apagado.

O valor padrão é `"1800"`.

`SUBVOLUME`

Ponto de montagem da partição ou do subvolume para o instantâneo. Não alterar.

`SYNC_ACL`

Se o Snapper for utilizado por usuários regulares (consulte a *Seção 4.4.1.2, "Usando o Snapper como usuário comum"*), eles deverão ter acesso e ler os arquivos dos diretórios `.snapshot`.

Se SYNC_ACL estiver definido como `yes`, o Snapper os tornará acessíveis automaticamente usando ACLs para usuários e grupos das entradas ALLOW_USERS ou ALLOW_GROUPS.

O valor padrão é `"no"`.

`TIMELINE_CLEANUP`

Define se é para apagar automaticamente os instantâneos antigos quando a quantidade exceder o número especificado com as opções *`TIMELINE_LIMIT_*`* *e* a duração especificada com `TIMELINE_MIN_AGE`. Valores válidos: `yes`, `no`
O valor padrão é `"no"`.

`TIMELINE_CREATE`

Se definido como `yes`, serão criados instantâneos por hora. No momento, esta é a única forma de criar instantâneos automaticamente, portanto, é altamente recomendável definilo como `yes`. Valores válidos: `yes`, `no`
O valor padrão é `"no"`.

`TIMELINE_LIMIT_DAILY`, `TIMELINE_LIMIT_HOURLY`, `TIMELINE_LIMIT_MONTHLY`, `TIMELINE_LIMIT_YEARLY`

Número de instantâneos para manter por hora, dia, mês, ano.
O valor padrão de cada entrada é `"10"`.

EXEMPLO 4.1 EXEMPLO DE CONFIGURAÇÃO DE LINHA DO TEMPO

```
TIMELINE_CLEANUP="yes"
TIMELINE_CREATE="yes"
TIMELINE_LIMIT_DAILY="10"
TIMELINE_LIMIT_HOURLY="10"
TIMELINE_LIMIT_MONTHLY="10"
TIMELINE_LIMIT_YEARLY="10"
TIMELINE_MIN_AGE="1800"
```

Este exemplo de configuração habilita os instantâneos por hora, que são limpos automaticamente. `TIMELINE_MIN_AGE` e `TIMELINE_LIMIT_*` são sempre avaliados juntos. Neste exemplo, a duração mínima de um instantâneo, antes de ser apagado, está definida como 30 minutos (1800 segundos). Como nós criamos instantâneos por hora, isso garante que apenas os instantâneos mais recentes sejam mantidos. Se `TIMELINE_LIMIT_DAILY` não estiver definido como zero, significa que o primeiro instantâneo do dia também será mantido.

INSTANTÂNEOS PARA MANTER

- De hora em hora: Os últimos dez instantâneos que foram criados.
- Diariamente: O primeiro instantâneo diário criado é mantido para os últimos dez dias.

- Mensalmente: O primeiro instantâneo criado no último dia do mês é mantido para os últimos dez meses.
- Anualmente: O primeiro instantâneo criado no último dia do ano é mantido para os últimos dez anos.

`TIMELINE_MIN_AGE`

Define a duração mínima em segundos do instantâneo antes de ser automaticamente apagado.
O valor padrão é `"1800"`.

4.4.1.2 Usando o Snapper como usuário comum

Por padrão, o Snapper só pode ser usado pelo `root`. No entanto, há casos em que determinados grupos ou usuários precisam criar instantâneos ou desfazer mudanças revertendo um instantâneo:

- administradores de site na Web que desejam criar instantâneos de `/srv/www`
- usuários que desejam criar instantâneo de seu diretório pessoal

Para essas finalidades, é possível criar configurações do Snapper que concedam permissões a usuários ou grupos. Os usuários especificados devem conseguir ler e acessar o diretório `.snapshots` correspondente. A maneira mais fácil de fazer isso é definir a opção SYNC_ACL como `yes`.

PROCEDIMENTO 4.5 HABILITANDO USUÁRIOS COMUNS A USAR O SNAPPER

Observe que todas as etapas deste procedimento devem ser executadas pelo `root`.

1. Se não houver um, crie uma configuração do Snapper para a partição ou o subvolume em que o usuário consiga utilizar o Snapper. Consulte a *Seção 4.4, "Criando e modificando as configurações do Snapper"* para obter instruções. Exemplo:

   ```
   snapper --config web_data create /srv/www
   ```

2. O arquivo de configuração é criado em `/etc/snapper/configs/CONFIG`, em que CONFIG é o valor que você especificou com `-c/--config` na etapa anterior (por exemplo, `/etc/snapper/configs/web_data`). Ajuste-o de acordo com as suas necessidades. Consulte a *Seção 4.4.1, "Gerenciando configurações existentes"* para obter os detalhes.

3. Defina os valores de `ALLOW_USERS` e `ALLOW_GROUPS` para conceder permissões a usuários e grupos, respectivamente. Separe várias entradas com `Space`. Para conceder permissões ao usuário `www_admin`, por exemplo, execute:

```
snapper -c web_data set-config "ALLOW_USERS=www_admin" SYNC_ACL="yes"
```

4. Agora o(s) usuário(s) e grupo(s) pode(m) utilizar a configuração especificada do Snapper. É possível testá-la com o comando `list`, por exemplo:

```
www_admin:~ > snapper -c web_data list
```

4.5 Criando e gerenciando instantâneos manualmente

Não é possível apenas criar e gerenciar os instantâneos automaticamente pela configuração do Snapper, você também pode criar pares de instantâneos (“antes e após”) ou instantâneos únicos manualmente usando a ferramenta de linha de comando ou o módulo do YaST.

Todas as operações do Snapper são executadas de acordo com uma configuração existente (consulte a *Seção 4.4, “Criando e modificando as configurações do Snapper”* para obter os detalhes). Você só pode criar instantâneos de partições ou volumes em que exista uma configuração. Por padrão, a configuração do sistema (`root`) é usada. Para criar ou gerenciar instantâneos com sua própria configuração, selecione-a de maneira clara. Use a caixa suspensa *Configuração Atual* no YaST ou especifique `-c` na linha de comando (**`snapper -c`** *`MINHACONFIG COMANDO`*).

4.5.1 Metadados de instantâneos

Cada instantâneo consiste no próprio instantâneo e em alguns metadados. Ao criar um instantâneo, você também precisa especificar os metadados. A modificação de um instantâneo também altera seus metadados; não é possível modificar seu conteúdo. Os seguintes metadados estão disponíveis para cada instantâneo:

- **Tipo**: Tipo do instantâneo, consulte a *Seção 4.5.1.1, “Tipos de instantâneos”* para obter os detalhes. Esses dados não podem ser mudados.
- **Número**: Número exclusivo do instantâneo. Esses dados não podem ser mudados.

- **Número do Pré**: Especifica o número do pré-instantâneo correspondente. Apenas para instantâneos do tipo pós. Esses dados não podem ser mudados.
- **Descrição**: A descrição do instantâneo.
- **Dados de usuário**: Uma descrição estendida que especifica os dados personalizados no formato de uma lista de chave=valor separada por vírgula: `reason=testing, project=foo`. Este campo também é usado para marcar um instantâneo como importante (`important=yes`) e listar o usuário que criou o instantâneo (user=tux).
- **Algoritmo de Limpeza**: Algoritmo de limpeza do instantâneo. Consulte a *Seção 4.5.1.2, "Algoritmos de limpeza"* para obter os detalhes.

4.5.1.1 Tipos de instantâneos

O Snapper reconhece três tipos diferentes de instantâneos: pre (pré), post (pós) e single (único). Eles são iguais fisicamente, mas o Snapper trabalha com eles de forma diferente.

`pre`
: Instantâneo de um sistema de arquivos *antes* da modificação. Cada instantâneo `pre` tem o seu `post` correspondente. Usado para os instantâneos automáticos do YaST/Zypper, por exemplo.

`post`
: Instantâneo de um sistema de arquivos *após* a modificação. Cada instantâneo `post` tem o seu `pre` correspondente. Usado para os instantâneos automáticos do YaST/Zypper, por exemplo.

`single`
: Instantâneo independente. Usado, por exemplo, para os instantâneos automáticos por hora. Esse é o tipo padrão quando se cria instantâneos.

4.5.1.2 Algoritmos de limpeza

O Snapper oferece três algoritmos para limpeza de instantâneos antigos. Os algoritmos são executados em uma tarefa cron diária. A frequência de limpeza é definida na configuração do Snapper para a partição ou o subvolume (consulte a *Seção 4.4.1, "Gerenciando configurações existentes"* para obter os detalhes).

number

Apaga instantâneos antigos quando determinado número de instantâneos é atingido.

timeline

Apaga instantâneos antigos que passaram de certa duração, mas mantém um número de instantâneos por hora, dia, mês e ano.

empty-pre-post

Apaga os pares de pré/pós-instantâneos com diffs vazias.

4.5.2 Criando instantâneos

A criação do instantâneo é feita executando o comando `snapper create` ou clicando em *Criar* no módulo *Snapper* do YaST. Os exemplos a seguir explicam como criar instantâneos da linha de comando. Eles são fáceis de adotar ao usar a interface do YaST.

Dica: Descrição do instantâneo

Especifique sempre uma descrição significativa para no futuro conseguir identificar sua finalidade. É possível especificar ainda mais informações na opção de dados do usuário.

`snapper create --description "Snapshot for week 2 2014"`

Cria um instantâneo independente (tipo único) na configuração padrão (`root`) com uma descrição. Como nenhum algoritmo de limpeza foi especificado, o instantâneo nunca será apagado automaticamente.

`snapper --config home create --description "Cleanup in ~tux"`

Cria um instantâneo independente (tipo único) em uma configuração personalizada chamada `home` com uma descrição. Como nenhum algoritmo de limpeza foi especificado, o instantâneo nunca será apagado automaticamente.

`snapper --config home create --description "Daily data backup" --cleanup-algorithm timeline`

Cria um instantâneo independente (tipo único) em uma configuração personalizada chamada `home` com uma descrição. O arquivo é apagado automaticamente quando atende aos critérios especificados no algoritmo de limpeza de linha do tempo da configuração.

`snapper create --type pre--print-number--description "Before the Apache config cleanup"--userdata "important=yes"`

Cria um instantâneo do tipo `pre` e imprime o número do instantâneo. Primeiro comando necessário para criar um par de instantâneos usado para gravar o estado “antes” e “após”. O instantâneo é marcado como importante.

`snapper create --type post--pre-number 30--description "After the Apache config cleanup"--userdata "important=yes"`

Cria um instantâneo do tipo `post` ligado a seu par `pre` de número `30`. Segundo comando necessário para criar um par de instantâneos usado para gravar o estado “antes” e “após”. O instantâneo é marcado como importante.

`snapper create --command COMANDO--description "Before and after COMANDO"`

Cria automaticamente um par de instantâneos antes e após a execução do *`COMANDO`*. Essa opção só está disponível ao usar o snapper na linha de comando.

4.5.3 Modificando os metadados do instantâneo

O Snapper permite modificar a descrição, o algoritmo de limpeza e os dados de usuário de um instantâneo. Todos os outros metadados não podem ser mudados. Os exemplos a seguir explicam como modificar instantâneos da linha de comando. Eles são fáceis de adotar ao usar a interface do YaST.

Para modificar um instantâneo na linha de comando, você precisa saber o número dele. Use `snapper list` para exibir todos os instantâneos e seus números.

O módulo *Snapper* do YaST já lista todos os instantâneos. Escolha um na lista e clique em *Modificar*.

`snapper modify --cleanup-algorithm "timeline" 10`

Modifica os metadados do instantâneo 10 na configuração padrão (`root`). O algoritmo de limpeza é definido como `timeline`.

`snapper --config home modify --description "daily backup" -cleanup-algorithm "timeline"120`

Modifica os metadados do instantâneo 120 na configuração personalizada chamada `home`. Uma nova descrição é definida e o algoritmo de limpeza fica indefinido.

4.5.4 Apagando instantâneos

Para apagar um instantâneo com o módulo *Snapper* do YaST, escolha-o na lista e clique em *Apagar*.

Para apagar um instantâneo com a ferramenta de linha de comando, você precisa saber o número dele. Para saber, execute **`snapper list`**. Para apagar um instantâneo, execute **`snapper delete`** *`NÚMERO`*.

Dica: Apagando pares de instantâneos

Ao apagar um instantâneo `pre`, sempre apague seu `post` correspondente (e vice-versa).

`snapper delete 65`

Apaga o instantâneo 65 na configuração padrão (`root`).

`snapper -c home delete 89 90`

Apaga os instantâneos 89 e 90 na configuração personalizada chamada `home`.

Dica: Apagar instantâneo sem referência

Às vezes, o instantâneo btrfs está presente, mas não o arquivo xml do **`snapper`** com os metadados. Portanto, para o **`snapper`**, o instantâneo não existe. Você precisa primeiro apagar o subvolume btrfs para poder apagar o diretório *`NÚMERO_DO_INSTANTÂNEO`*:

```
btrfs subvolume delete /.snapshots/SNAPSHOTNUMBER/snapshot
    rm -rf /.snapshots/SNAPSHOTNUMBER
```

Dica: Instantâneos antigos ocupam mais espaço em disco

Se você apagar instantâneos para liberar espaço no disco rígido, apague primeiro os instantâneos antigos. Quanto mais antigo for o instantâneo, mais espaço em disco ele ocupa.

Os instantâneos também são automaticamente apagados por uma tarefa cron diária. Consulte a *Seção 4.5.1.2, "Algoritmos de limpeza"* para obter os detalhes.

4.6 Perguntas mais frequentes

P: Por que o Snapper nunca mostra as mudanças em `/var/log`, `/tmp` e em outros diretórios?

R: Para alguns diretórios, nós decidimos excluí-los dos instantâneos. Consulte *Diretórios que são excluídos dos instantâneos* para ver a lista e os motivos. Para excluir um caminho dos instantâneos, nós criamos um subvolume para esse caminho.

P: Quanto espaço no disco está sendo usado por instantâneos? Como liberar espaço no disco?

R: Como o **`df`** não mostra a utilização do disco correta nos sistemas de arquivos `Btrfs`, você precisa usar o comando **`btrfs filesystem df`** *`PONTO_DE_MONTAGEM`*. A exibição da quantidade de espaço em disco alocada por um instantâneo não é suportada pelas ferramentas do `Btrfs`.

Para liberar espaço em uma partição do `Btrfs` com instantâneos, é preciso apagar instantâneos desnecessários, e não arquivos. Os instantâneos antigos ocupam mais espaço do que os novos. Consulte a *Seção 4.1.1.3, "Controlando o armazenamento de instantâneos"* para obter os detalhes.

O upgrade de um service pack para outro resulta em instantâneos que ocupam muito espaço em disco nos subvolumes do sistema, porque muitos dados são modificados (atualizações de pacotes). É recomendada a exclusão manual dos instantâneos quando eles não são mais necessários. Consulte a *Seção 4.5.4, "Apagando instantâneos"* para obter os detalhes.

P: Posso inicializar um instantâneo do carregador de boot?

R: Sim, veja os detalhes na *Seção 4.3, "Rollback do sistema por inicialização de instantâneos"*.

P: Onde encontro mais informações sobre o Snapper?

R: Consulte a home page do Snapper em http://snapper.io/.

5 Acesso remoto com VNC

O VNC (Virtual Network Computing) permite controlar um computador remoto por uma área de trabalho gráfica (ao contrário do acesso remoto a shell). O VNC é independente de plataforma e permite acessar a máquina remota de qualquer sistema operacional.

O SUSE Linux Enterprise Desktop suporta dois tipos diferentes de sessões VNC: sessões únicas, que permanecem "ativas" enquanto a conexão VNC do cliente está ativada, e sessões persistentes, que permanecem "ativas" até serem explicitamente terminadas.

Nota: Tipos de sessão

Uma máquina é capaz de oferecer ambos os tipos de sessões simultaneamente em portas diferentes, mas uma sessão aberta não pode ser convertida de um tipo em outro.

5.1 Sessões VNC únicas

Uma sessão única é iniciada por um cliente remoto. Ela inicia uma tela gráfica de login no servidor. Desse modo, você pode escolher o usuário que inicia a sessão e, se suportado pelo gerenciador de login, o ambiente de área de trabalho. Após terminar a conexão do cliente para essa sessão VNC, todos os aplicativos iniciados nessa sessão também serão terminados. Sessões VNC únicas não podem ser compartilhadas, mas é possível ter várias sessões em um único host ao mesmo tempo.

PROCEDIMENTO 5.1 HABILITANDO SESSÕES VNC ÚNICAS

1. Inicie o *YaST › Serviços de Rede › Administração Remota (VNC)*.
2. Marque *Permitir Administração Remota*.
3. Se necessário, marque também *Abrir Porta no Firewall* (por exemplo, quando a interface de rede estiver configurada para ficar na Zona Externa). Se você tem mais de uma interface de rede, restrinja a abertura de portas no firewall a uma interface específica em *Detalhes do Firewall*.
4. Confirme as suas configurações clicando em *Concluir*.
5. Caso nem todos os pacotes necessários já estejam disponíveis, aprove a instalação dos pacotes ausentes.

Nota: Configurações disponíveis

A configuração padrão no SUSE Linux Enterprise Desktop confere às sessões uma resolução de 1024 x 768 pixels com profundidade de cores de 16 bits. As sessões estão disponíveis nas portas `5901` para viewers VNC “regulares” (equivalente à exibição VNC `1`) e na porta `5801` para browsers da Web.

É possível disponibilizar outras configurações em portas diferentes. Pergunte ao administrador do sistema.

Os números de exibição VNC e os números de exibição X são independentes nas sessões únicas. Um número de exibição VNC é atribuído manualmente a todas as configurações suportadas pelo servidor (:1 no exemplo acima). Sempre que uma sessão VNC é iniciada com uma das configurações, ela recebe automaticamente um número de exibição X livre.

5.1.1 Iniciando uma sessão VNC única

Para iniciar uma sessão VNC única, é preciso instalar um viewer VNC na máquina cliente. O viewer padrão dos produtos SUSE Linux é **`vncviewer`**, incluído no pacote `tigervnc` (padrão) ou, alternativamente, no pacote `tightvnc`. É possível também ver uma sessão VNC pelo browser da Web e por um applet Java.

Para iniciar seu viewer VNC e iniciar uma sessão com a configuração padrão do servidor, use o comando:

```
vncviewer jupiter.example.com:1
```

Em vez do número de exibição do VNC, você também pode especificar o número da porta com dois-pontos duplos:

```
vncviewer jupiter.example.com::5901
```

Se preferir, use um browser da Web compatível com Java para ver a sessão VNC digitando o seguinte URL: `http://jupiter.example.com:5801`

5.1.2 Configurando sessões VNC únicas

Você poderá ignorar esta seção se não precisar nem desejar modificar a configuração padrão.

As sessões VNC únicas são iniciadas pelo daemon `xinetd`. Um arquivo de configuração está localizado em `/etc/xinetd.d/vnc`. Por padrão, ele oferece seis blocos de configuração: três para viewers VNC (`vnc1` a `vnc3`) e três para atender a um applet Java (`vnchttpd1` a `vnchttpd3`). Por padrão, apenas `vnc1` e `vnchttpd1` estão ativos.

Para ativar uma configuração, comente a linha `disable = yes` com o caractere `#` na primeira coluna ou remova totalmente essa linha. Para desativar uma configuração, remova o comentário ou adicione a linha.

O servidor **`Xvnc`** pode ser configurado pela opção `server_args`. Consulte **`Xnvc --help`** para obter a lista de opções.

Ao adicionar configurações padrão, certifique-se de que elas não usem portas já em uso por outras configurações, outros serviços ou sessões VNC persistentes existentes no mesmo host.

Ative as mudanças na configuração digitando o seguinte comando:

```
sudo rcxinetd reload
```

Importante: Firewall e portas VNC

Ao ativar a Administração Remota conforme descrito no *Procedimento 5.1, "Habilitando sessões VNC únicas"*, as portas `5801` e `5901` são abertas no firewall. Se a interface de rede que atende às sessões VNC for protegida por firewall, será necessário abrir manualmente as respectivas portas ao ativar portas adicionais para as sessões VNC. Consulte o *Book "Security Guide" 15 "Masquerading and Firewalls"* para obter instruções.

5.2 Sessões VNC persistentes

Uma sessão VNC persistente é iniciada no servidor. A sessão e todos os aplicativos iniciados nessa sessão são executados independentemente das conexões do cliente até a sessão ser terminada.

É possível acessar uma sessão persistente de vários clientes ao mesmo tempo. Isso é ideal para fins de demonstração em que um cliente tem acesso total, e todos os outros têm acesso apenas exibição. Outro cenário de uso são treinamentos em que o instrutor pode precisar acessar a área de trabalho do aluno. Mas, na maioria das vezes, você possivelmente não vai querer compartilhar sua sessão VNC.

Ao contrário das sessões únicas que iniciam um gerenciador de exibição, uma sessão persistente inicia uma área de trabalho pronta para funcionar executada como o usuário que iniciou a sessão VNC.

O acesso às sessões persistentes é protegido por dois tipos de senhas possíveis:

- uma senha regular que permite acesso total ou
- uma senha opcional apenas exibição que permite acesso não interativo (apenas exibição).

Uma sessão pode ter várias conexões de cliente de ambos os tipos de uma só vez.

PROCEDIMENTO 5.2 INICIANDO UMA SESSÃO VNC PERSISTENTE

1. Abra um shell e verifique se você está conectado como o usuário proprietário da sessão VNC.
2. Se a interface de rede que atende às sessões VNC for protegida por firewall, será necessário abrir manualmente a porta usada pela sessão no firewall. Se você iniciar várias sessões, poderá também abrir uma faixa de portas. Consulte o *Book* "Security Guide" *15 "Masquerading and Firewalls"* para obter os detalhes sobre como configurar o firewall.
   O **`vncserver`** usa as portas `5901` para exibição `:1`, `5902` para exibição `:2`, e assim por diante. Para sessões persistentes, a exibição VNC e a exibição X geralmente têm o mesmo número.
3. Para iniciar uma sessão com resolução de 1024 x 769 pixels e profundidade de cores de 16 bits, digite o seguinte comando:

   ```
   vncserver -geometry 1024x768 -depth 16
   ```

   O comando **`vncserver`** escolhe um número de exibição não usado quando nenhum número é especificado e imprime essa escolha. Consulte **`man 1 vncserver`** para ver mais opções.

Quando você executa o **`vncviewer`** pela primeira vez, ele pede uma senha para acesso total à sessão. Se necessário, forneça também uma senha de acesso apenas exibição à sessão.

A(s) senha(s) inserida(s) aqui também será(ão) usada(s) em sessões futuras iniciadas pelo mesmo usuário. Elas podem ser modificadas com o comando **`vncpasswd`**.

Importante: Considerações sobre segurança

Verifique se está usando senhas avançadas de tamanho significativo (oito ou mais caracteres). Não compartilhe essas senhas.

As conexões VNC não são criptografadas, portanto, quem conseguir detectar a(s) rede(s) entre as duas máquinas poderá ler a senha quando ela for transferida no início de uma sessão.

Para terminar a sessão, encerre o ambiente de área de trabalho executado na sessão VNC pelo viewer do VNC, da mesma forma que você encerra uma sessão X local regular.

Se preferir terminar a sessão manualmente, abra um shell no servidor VNC e certifique-se de estar conectado como o usuário que possui a sessão VNC que deseja terminar. Execute o seguinte comando para terminar a sessão em execução na exibição `:1`: **`vncserver -kill :1`**

5.2.1 Conectando-se a uma sessão VNC persistente

Para conectar-se a uma sessão VNC persistente, é preciso instalar o viewer do VNC. O viewer padrão dos produtos SUSE Linux é **`vncviewer`**, incluído no pacote `tigervnc` (padrão) ou, alternativamente, no pacote `tightvnc`. É possível também ver uma sessão VNC pelo browser da Web e por um applet Java.

Para iniciar o viewer do VNC e conectar-se à exibição `:1` do servidor VNC, use o comando

```
vncviewer jupiter.example.com:1
```

Em vez do número de exibição do VNC, você também pode especificar o número da porta com dois-pontos duplos:

```
vncviewer jupiter.example.com::5901
```

Se preferir, use um browser da Web compatível com Java para ver a sessão VNC digitando o seguinte URL: `http://jupiter.example.com:5801`

5.2.2 Configurando sessões VNC persistentes

É possível configurar as sessões VNC persistentes editando `$HOME/.vnc/xstartup`. Por padrão, o script shell inicia o mesmo gerenciador de janelas/GUI do qual ele foi iniciado. No SUSE Linux Enterprise Desktop, pode ser o GNOME ou o IceWM. Para iniciar a sessão com um gerenciador de janelas de sua escolha, defina a variável `WINDOWMANAGER`:

```
WINDOWMANAGER=gnome vncserver -geometry 1024x768
WINDOWMANAGER=icewm vncserver -geometry 1024x768
```

Nota: Uma configuração para cada usuário

Sessões VNC persistentes são configuradas em uma única configuração por usuário. Várias sessões iniciadas pelo mesmo usuário utilizarão todos os mesmos arquivos de inicialização e senha.

6 Configuração do GNOME para administradores

Este capítulo introduz as opções de configuração do GNOME que os administradores podem usar para definir ajustes em todo o sistema, como personalização de menus, instalação de temas, configuração de fontes, mudança dos aplicativos preferidos e bloqueio de recursos.

Essas opções de configuração estão armazenadas no sistema GConf. Acesse o sistema GConf usando ferramentas como a interface de linha de comando **`gconftool-2`** ou a interface gráfica do usuário **`gconf-editor`**.

6.1 Iniciando aplicativos automaticamente

Para iniciar aplicativos automaticamente no GNOME, use um dos seguintes métodos:

- **Para executar aplicativos para cada usuário:** coloque os arquivos `.desktop` em `/usr/share/gnome/autostart`.
- **Para executar aplicativos para um único usuário:** coloque os arquivos `.desktop` em `~/.config/autostart`.

Para desabilitar um aplicativo que é iniciado automaticamente, adicione `X-Autostart-enabled=false` ao arquivo `.desktop`.

6.2 Montando automaticamente e gerenciando dispositivos de mídia

O Nautilus (**`nautilus`**) monitora eventos relacionados a volume e responde com uma política especificada pelo usuário. Você pode usar o Nautilus para montar automaticamente as unidades de hot plug e a mídia removível inserida, executar programas automaticamente e reproduzir CDs de áudio ou DVDs de vídeo. O Nautilus também pode importar automaticamente fotos de uma câmera digital.

Os administradores do sistema podem definir padrões para todo o sistema. Para obter mais informações, consulte a *Seção 6.3, “Mudando os aplicativos preferenciais”*.

6.3 Mudando os aplicativos preferenciais

Para mudar os aplicativos preferenciais dos usuários, edite `/etc/gnome_defaults.conf`. Mais dicas são encontradas neste arquivo.

Para obter mais informações sobre tipos MIME, consulte http://www.freedesktop.org/Standards/shared-mime-info-spec.

6.4 Adicionando modelos de documentos

Para disponibilizar modelos de documentos aos usuários, insira-os no diretório `Templates` no diretório pessoal de um usuário. Isso pode ser feito manualmente para cada usuário, copiando-se os arquivos para `~/Templates`, ou para todo o sistema, adicionando-se um diretório `Templates` com documentos a `/etc/skel` antes que o usuário seja criado.

Um usuário cria um novo documento a partir de um modelo clicando o botão direito do mouse na área de trabalho e selecionando *Criar Documento*.

6.5 Para obter mais informações

Para obter mais informações, consulte http://help.gnome.org/admin/.

7 Gerenciando software com ferramentas de linha de comando

Este capítulo descreve o Zypper e o RPM, duas ferramentas de linha de comando para gerenciar software. Para obter a definição da terminologia usada neste contexto (por exemplo, `repositório`, `patch` ou `atualização`), consulte a *Book "*Deployment Guide*" 6 "Installing or Removing Software"6.1 "Definition of Terms"*.

7.1 Usando o zypper

O zypper é um gerenciador de pacotes de linha de comando para instalar, atualizar e remover pacotes, bem como para gerenciar repositórios. Ele é especialmente útil para realizar tarefas de gerenciamento remoto de software ou gerenciar software de scripts de shell.

7.1.1 Uso geral

A sintaxe geral do zypper é:

```
zypper [--global-options] command  [--command-options] [arguments]
  ...
```

Os componentes entre colchetes não são obrigatórios. Consulte **`zypper help`** para obter uma lista de opções gerais e todos os comandos. Para obter ajuda sobre determinado comando, digite **`zypper help`** *`comando`*.

A maneira mais simples de executar o zypper é digitar seu nome seguido de um comando. Por exemplo, para aplicar todos os patches necessários ao sistema, digite:

```
zypper patch
```

Você também pode escolher dentre uma ou mais opções globais, digitando-as logo antes do comando. Por exemplo, `--non-interactive` significa executar o comando sem perguntar nada (aplicando as respostas padrão automaticamente):

```
zypper --non-interactive patch
```

Para usar as opções específicas de um comando em particular, digite-as logo após o comando. Por exemplo, `--auto-agree-with-licenses` significa aplicar todos os patches necessários ao sistema sem solicitar confirmação de nenhuma licença (eles serão aceitos automaticamente):

```
zypper patch --auto-agree-with-licenses
```

Alguns comandos requerem um ou mais argumentos. Ao usar o comando install, por exemplo, é preciso especificar o(s) pacotes(s) a instalar:

```
zypper install mplayer
```

Algumas opções também requerem um argumento. O comando a seguir lista todos os padrões conhecidos:

```
zypper search -t pattern
```

Você pode combinar todos os anteriores. Por exemplo, o comando a seguir instala os pacotes `aspell-de` e `aspell-fr` do repositório `factory` durante o modo verboso:

```
zypper -v install --from factory aspell-de aspell-fr
```

A opção `--from` trata de manter todos os repositórios habilitados (para resolução de dependências) enquanto solicita o pacote do repositório especificado.

Quase todos os comandos zypper possuem uma opção `dry-run` que simula o comando indicado. Ela pode ser usada para fins de teste.

```
zypper remove --dry-run MozillaFirefox
```

O Zypper suporta a opção global `--userdata` *`string`*. É possível especificar uma string com essa opção, que é gravada nos arquivos de registro e plug-ins do Zypper (como o plug-in Btrfs). Ela pode ser usada para marcar e identificar transações nos arquivos de registro.

```
zypper --userdata string patch
```

7.1.2 Instalando e removendo software com o zypper

Para instalar ou remover pacotes, use os seguintes comandos:

```
zypper install package_name
zypper remove package_name
```

O zypper conhece várias maneiras de tratar pacotes para os comandos install e remove.

pelo nome exato do pacote (e número da versão)

```
zypper install MozillaFirefox
```

ou

```
zypper install MozillaFirefox-3.5.3
```

pelo álias do repositório e pelo nome do pacote

```
zypper install mozilla:MozillaFirefox
```

onde `mozilla` é o álias do repositório a partir do qual instalar.

pelo nome do pacote usando curingas

O comando a seguir instalará todos os pacotes cujos nomes começam com “Moz”. Use-o com cuidado, principalmente ao remover pacotes.

```
zypper install 'Moz*'
```

por recurso

Por exemplo, para instalar um módulo Perl sem saber o nome do pacote, os recursos podem ser convenientes:

```
zypper install firefox
```

por recurso e/ou arquitetura e/ou versão

Juntamente com um recurso, você pode especificar a arquitetura (como `x86_64`) e/ou a versão. A versão deve ser precedida por um operador: `<` (menor que), `<=` (menor que ou igual), `=` (igual), `>=` (maior que ou igual), `>` (maior que).

```
zypper install 'firefox.x86_64'
```

```
zypper install 'firefox>=3.5.3'
zypper install 'firefox.x86_64>=3.5.3'
```

por caminho para o arquivo RPM

Você também pode especificar um local ou caminho remoto para um pacote:

```
zypper install /tmp/install/MozillaFirefox.rpm
zypper install http://download.opensuse.org/repositories/mozilla/SUSE_Factory/
x86_64/MozillaFirefox-3.5.3-1.3.x86_64.rpm
```

Para instalar e remover pacotes simultaneamente, use os modificadores `+/-`. Para instalar o `emacs` e remover o `vim` simultaneamente, use:

```
zypper install emacs -vim
```

Para remover o `emacs` e instalar o `vim` simultaneamente, use:

```
zypper remove emacs +vim
```

Para impedir que o nome do pacote iniciado por `-` seja interpretado como uma opção de comando, use-o sempre como segundo argumento. Se isso não for possível, preceda-o com `--`:

```
zypper install -emacs +vim       # Wrong
zypper install vim -emacs        # Correct
zypper install -- -emacs +vim    # same as above
zypper remove emacs +vim         # same as above
```

Para (com determinado pacote) remover automaticamente qualquer pacote desnecessário após remover o pacote especificado, use a opção `--clean-deps`:

```
zypper rm package_name --clean-deps
```

Por padrão, o zypper solicita uma confirmação antes de instalar ou remover um pacote selecionado, ou quando ocorre um problema. Você pode anular esse comportamento usando a opção `--non-interactive`. Essa opção deve ser inserida antes do comando real (**`install`**, **`remove`** e **`patch`**), conforme mostrado a seguir:

```
zypper --non-interactive install package_name
```

Essa opção permite o uso do zypper em scripts e tarefas cron.

Atenção: não remova pacotes de sistema obrigatórios

Não remova pacotes como `glibc`, `zypper`, `kernel` ou similares. Esses pacotes são obrigatórios para o sistema e, se removidos, podem fazer o sistema ficar instável ou parar de funcionar de vez.

7.1.2.1 Instalando ou fazendo download dos pacotes de origem

Se desejar instalar o pacote de origem de um pacote, use:

```
zypper source-install package_name
```

Esse comando também instalará as dependências de compilação do pacote especificado. Se não quiser isso, adicione o switch `-D`. Para instalar apenas as dependências de compilação, use `-d`.

```
zypper source-install -D package_name # source package only
zypper source-install -d package_name # build dependencies only
```

Naturalmente isso só funcionará se o repositório com os pacotes de origem estiver habilitado na sua lista de repositórios (ele é adicionado por padrão, mas não habilitado). Consulte a *Seção 7.1.4, "Gerenciando repositórios com o zypper"* para obter os detalhes sobre o gerenciamento de repositórios.

Uma lista de todos os pacotes de origem disponíveis nos seus repositórios pode ser obtida com:

```
zypper search -t srcpackage
```

É possível também fazer download dos pacotes de origem para todos os pacotes instalados em um diretório local. Para fazer download dos pacotes de origem, use:

```
zypper source-download
```

O diretório de download padrão é `/var/cache/zypper/source-download`. Você pode mudá-lo usando a opção `--directory`. Para mostrar apenas os pacotes ausentes ou incorretos sem fazer download nem apagar nada, use a opção `--status`. Para apagar pacotes de origem incorretos, use a opção `--delete`. Para desabilitar a exclusão, use a opção `--no-delete`.

7.1.2.2 Utilitários

Para verificar se todas as dependências ainda são atendidas e para reparar dependências ausentes, use:

```
zypper verify
```

Além das dependências que precisam ser atendidas, alguns pacotes "recomendam" outros pacotes. Esses pacotes recomendados são instalados apenas quando estão realmente disponíveis e são instaláveis. Caso os pacotes recomendados fiquem disponíveis após a instalação do pacote que os recomendou (adicionando outros pacotes ou hardware), use o seguinte comando:

```
zypper install-new-recommends
```

Este comando será muito útil após conectar uma webcam ou um dispositivo Wi-Fi. Ele instala drivers para o dispositivo e software relacionado, se disponíveis. Os drivers e o software relacionado serão instaláveis se determinadas dependências de hardware forem atendidas.

7.1.3 Atualizando software com o zypper

Existem três maneiras diferentes de atualizar o software usando o zypper: instalando patches, instalando uma versão nova de um pacote ou atualizando a distribuição inteira. Para a segunda opção, use o comando **`zypper dist-upgrade`**. O upgrade do SUSE Linux Enterprise Desktop é discutido no *Book "*Deployment Guide*" 4 "Updating SUSE Linux Enterprise"*.

7.1.3.1 Instalando patches

Para instalar todos os patches lançados oficialmente que se aplicam ao seu sistema, execute:

```
zypper patch
```

Nesse caso, todos os patches disponíveis em seus repositórios são verificados quanto à sua relevância e instalados, se necessário. Após o registro de sua instalação do SUSE Linux Enterprise Desktop, um repositório de atualização oficial contendo os patches será adicionado ao seu sistema. O comando acima é tudo o que você deve digitar para aplicá-los quando necessário.

O zypper conhece três comandos diferentes para consultar a disponibilidade dos patches:

`zypper patch-check`

Lista o número de patches necessários (patches que se aplicam ao seu sistema e ainda não estão instalados)

```
tux > sudo zypper patch-check
Loading repository data...
Reading installed packages...
5 patches needed (1 security patch)
```

`zypper list-patches`

Lista todos os patches necessários (patches que se aplicam ao seu sistema e ainda não estão instalados)

```
tux > sudo zypper list-patches
Loading repository data...
Reading installed packages...

Repository     | Name        | Version | Category | Status  | Summary
---------------+-------------+---------+----------+---------+---------
SLES12-Updates | SUSE-2014-8 | 1       | security | needed  | openssl: Update to OpenSSL 1.0.1g
```

`zypper patches`

Lista todos os patches disponíveis para o SUSE Linux Enterprise Desktop, independentemente de já estarem instalados ou de se aplicarem à sua instalação.

Também é possível listar e instalar todos os patches relevantes a problemas específicos. Para listar patches específicos, use o comando **`zypper list-patches`** com as seguintes opções:

`--bugzilla[=`*`número`*`]`

Lista todos os patches necessários para problemas do Bugzilla. Opcionalmente, você pode inserir um número de bug para listar apenas os patches para esse bug específico.

`--cve[=número]`

Lista todos os patches necessários para problemas do CVE (Common Vulnerabilities and Exposures) ou apenas os patches correspondentes a determinado número de CVE, se especificado.

Para instalar um patch para um problema específico do Bugzilla ou do CVE, use os seguintes comandos:

```
zypper patch --bugzilla=number
```

ou

```
zypper patch --cve=number
```

Por exemplo, para instalar um patch de segurança com o número do CVE `CVE-2010-2713`, execute:

```
zypper patch --cve=CVE-2010-2713
```

7.1.3.2 Instalando novas versões de pacotes

Se um repositório contém apenas pacotes novos, mas não fornece patches, **`zypper patch`** não surte nenhum efeito. Para atualizar todos os pacotes instalados com as versões mais recentes disponíveis (sem afetar a integridade do sistema), use:

```
zypper update
```

Para atualizar pacotes individuais, especifique o pacote com o comando update ou install:

```
zypper update package_name
zypper install package_name
```

Uma lista de todos os novos pacotes instaláveis pode ser obtida pelo comando:

```
zypper list-updates
```

Observe que este comando apenas lista os pacotes correspondentes aos seguintes critérios:

- têm os mesmo fornecedor que o pacote já instalado,
- são fornecidos por repositórios com pelo menos a mesma prioridade que o pacote já instalado,
- são instaláveis (todas as dependências foram atendidas).

Uma lista de *todos* os novos pacotes disponíveis (sejam instaláveis ou não) pode ser obtida com:

```
zypper list-updates --all
```

Para descobrir o motivo pelo qual um novo pacote não pode ser instalado, use o comando **`zypper install`** ou **`zypper update`** conforme descrito acima.

7.1.4 Gerenciando repositórios com o zypper

Todos os comandos de instalação ou patch do zipper dependem de uma lista de repositórios conhecidos. Para listar todos os repositórios conhecidos para o sistema, use o comando:

```
zypper repos
```

O resultado parecerá com o seguinte:

EXEMPLO 7.1 ZYPPER: LISTA DE REPOSITÓRIOS CONHECIDOS

```
# | Alias        | Name          | Enabled | Refresh
--+--------------+---------------+---------+--------
1 | SLEHA-12-GEO | SLEHA-12-GEO  | Yes     | No
2 | SLEHA-12     | SLEHA-12      | Yes     | No
3 | SLES12       | SLES12        | Yes     | No
```

Na especificação de repositórios em vários comandos, é possível usar um álias, URI ou número de repositório a partir da saída do comando **`zypper repos`**. O álias do repositório é uma versão abreviada do nome do repositório para uso em comandos de gerenciamento de repositórios. Observe que os números dos repositórios podem ser mudados após modificar a lista de repositórios. O álias nunca mudará sozinho.

Por padrão; detalhes, como o URI ou a prioridade do repositório, não são exibidos. Use o seguinte comando para listar todos os detalhes:

```
zypper repos -d
```

7.1.4.1 Adicionando repositórios

Para adicionar um repositório, execute

```
zypper addrepo URI alias
```

O *`URI`* pode ser um repositório da Internet, um recurso de rede, um diretório ou um CD ou DVD (consulte http://en.opensuse.org/openSUSE:Libzypp_URIs para obter os detalhes). O *`álias`* é um identificador abreviado e exclusivo do repositório. Você tem livre escolha, com a única condição de que seja exclusivo. O zypper emitirá um aviso se você especificar um álias que já está em uso.

7.1.4.2 Removendo repositórios

Se você deseja remover um repositório da lista, use o comando **`zypper removerepo`** junto com o álias ou o número do repositório que você deseja apagar. Por exemplo, para remover o repositório `SLEHA-12-GEO` do *Exemplo 7.1, "Zypper: lista de repositórios conhecidos"*, use um dos seguintes comandos:

```
zypper removerepo 1
zypper removerepo "SLEHA-12-GEO"
```

7.1.4.3 Modificando repositórios

Habilite ou desabilite os repositórios com **`zypper modifyrepo`**. Você também pode alterar as propriedades do repositório (por exemplo, atualizar o comportamento, o nome ou a prioridade) com esse comando. O comando a seguir habilita o repositório chamado `updates`, ativa a atualização automática e define sua prioridade como 20:

```
zypper modifyrepo -er -p 20 'updates'
```

A modificação de repositórios não se limita a um único repositório, você também pode operar em grupos:

`-a`: todos os repositórios
`-l`: repositórios locais
`-t`: repositórios remotos
`-m` *`TIPO`*: repositórios de um tipo específico (em que *`TIPO`* pode ser um dos seguintes: `http`, `https`, `ftp`, `cd`, `dvd`, `dir`, `file`, `cifs`, `smb`, `nfs`, `hd`, `iso`)

Para renomear o álias de um repositório, use o comando `renamerepo`. O exemplo a seguir muda o álias de `Mozilla Firefox` para `firefox`:

```
zypper renamerepo 'Mozilla Firefox' firefox
```

7.1.5 Consultando repositórios e pacotes com o zypper

O zypper oferece vários métodos de consulta a repositórios ou pacotes. Para obter as listas de todos os produtos, padrões, pacotes ou patches disponíveis, use os seguintes comandos:

```
zypper products
zypper patterns
zypper packages
zypper patches
```

Para consultar todos os repositórios para determinados pacotes, use `search`. Ela funciona em nomes de pacotes ou, opcionalmente, em resumos e descrições de pacotes. Uma string entre `/` é interpretada como expressão regular. Por padrão, a pesquisa não diferencia maiúsculas de minúsculas.

Pesquisa simples de nome de pacote que inclua `fire`

```
zypper search "fire"
```

Pesquisa simples do pacote exato `MozillaFirefox`

```
zypper search --match-exact "MozillaFirefox"
```

Pesquisar também em descrições e resumos de pacotes

```
zypper search -d fire
```

Exibir apenas pacotes ainda não instalados

```
zypper search -u fire
```

Exibir pacotes que tenham a string `fir`, não seguida por `e`

zypper se "/fir[^e]/"

Para procurar pacotes que oferecem um recurso específico, use o comando `what-provides`. Por exemplo, para saber qual pacote inclui o módulo Perl `SVN::Core`, use o seguinte comando:

```
zypper what-provides 'perl(SVN::Core)'
```

Para consultar pacotes únicos, use **`info`** com um nome exato de pacote como argumento. Ele exibe informações detalhadas sobre um pacote. Para mostrar também o que é exigido/recomendado pelo pacote, use as opções `--requires` e `--recommends`:

```
zypper info --requires MozillaFirefox
```

O `what-provides` *`pacote`* é semelhante a **`rpm -q --whatprovides`** *`pacote`*, mas o RPM só pode consultar o banco de dados RPM (que é o banco de dados de todos os pacotes instalados). O zypper, por outro lado, o informará sobre fornecedores do recurso a partir de qualquer repositório, não apenas aqueles que estão instalados.

7.1.6 Configurando o Zypper

O Zypper agora vem com um arquivo de configuração que permite mudar permanentemente o comportamento do Zypper (de todo o sistema ou de um usuário específico). Para mudanças de todo o sistema, edite `/etc/zypp/zypper.conf`. Para mudanças específicas do usuário, edite `~/.zypper.conf`. Se `~/.zypper.conf` ainda não existir, você poderá usar `/etc/zypp/zypper.conf` como gabarito: copie-o para `~/.zypper.conf` e ajuste-o como desejar. Consulte os comentários no arquivo para obter ajuda sobre as opções disponíveis.

7.1.7 Solucionando problemas

Caso tenha problemas para acessar os pacotes dos repositórios configurados (por exemplo, o Zypper não encontra determinado pacote apesar de você saber que ele existe em um dos repositórios), poderá ajudar se você atualizar os repositórios com:

```
zypper refresh
```

Se isso não ajudar, tente

```
zypper refresh -fdb
```

Isso força uma atualização completa e a reconstrução do banco de dados, incluindo um download forçado dos metadados iniciais.

7.1.8 Recurso de rollback do Zypper no sistema de arquivos Btrfs

Se o sistema de arquivos Btrfs for usado na partição raiz e o **`snapper`** estiver instalado, o Zypper chamará automaticamente o **`snapper`** (usando o script instalado pelo **`snapper`**) ao confirmar as mudanças no sistema de arquivos para criar os instantâneos apropriados do sistema de arquivos.

É possível usar esses instantâneos para reverter as mudanças feitas pelo Zypper. Consulte o *Capítulo 4, Recuperação de sistema e gerenciamento de instantâneos com o Snapper* para obter mais informações.

7.1.9 Para obter mais informações

Para obter mais informações sobre como gerenciar o software da linha de comando, digite **`zypper help`**, **`zypper help`** *`comando`* ou consulte a página de manual de `zypper(8)`. Para obter uma referência completa e detalhada dos comandos, incluindo `folhetos de dicas` com os comandos mais importantes, e informações sobre como usar o Zypper em scripts e aplicativos, consulte http://en.opensuse.org/SDB:Zypper_usage. Você encontra uma lista das mudanças de software da versão mais recente do SUSE Linux Enterprise Desktop em http://en.opensuse.org/openSUSE:Zypper versions.

7.2 RPM — o gerenciador de pacotes

O RPM (gerenciador de pacotes RPM) é usado para gerenciar pacotes de software. Seus principais comandos são **`rpm`** e **`rpmbuild`**. O banco de dados RPM avançado pode ser consultado pelos usuários, administradores de sistema e construtores de pacotes para obtenção de informações detalhadas sobre o software instalado.

Basicamente, o **`rpm`** possui cinco modos: instalação, desinstalação (ou atualização) de pacotes de software, reconstrução do banco de dados RPM, consulta de bancos RPM ou arquivos RPM individuais, verificação de integridade dos pacotes e assinatura de pacotes. O **`rpmbuild`** pode ser usado para construir pacotes instaláveis de fontes originais.

Os arquivos RPM instaláveis são compactados em um formato binário especial. Esses são arquivos de programa para instalação e determinadas metainformações usadas durante a instalação pelo comando **rpm** para configurar o pacote de softwares. Também são armazenados no banco de dados RPM com o objetivo de documentação. Os arquivos RPM normalmente têm a extensão `.rpm`.

Dica: pacotes de desenvolvimento de software

Para vários pacotes, os componentes necessários para o desenvolvimento de software (bibliotecas, cabeçalhos, arquivos de inclusão etc.) foram colocados em pacotes separados. Esses pacotes de desenvolvimento só são necessários quando você deseja compilar software por conta própria (por exemplo, os pacotes do GNOME mais recentes). É possível identificá-los pela extensão do nome `-devel`, como os pacotes `alsa-devel` e `gimp-devel`.

7.2.1 Verificando a autenticidade do pacote

Os pacotes RPM têm uma assinatura GPG. Para verificar a assinatura de um pacote RPM, use o comando **rpm --checksig** *pacote*-1.2.3.rpm para determinar se o pacote vem do SUSE ou de outro recurso confiável. Isso é especialmente recomendado para pacotes de atualização da Internet.

7.2.2 Gerenciando pacotes: instalar, atualizar e desinstalar

Normalmente, a instalação de um arquivo RPM é bem simples: **rpm -i** *pacote*.rpm. Com esse comando, o pacote é instalado, mas apenas quando suas dependências são atendidas e quando não há conflitos com outros pacotes. Com uma mensagem de erro, o **rpm** solicita os pacotes que devem ser instalados para atender a requisitos de dependência. No segundo plano, o banco de dados RPM garante que não haja conflitos, pois um arquivo específico pode pertencer somente a

um pacote. Ao escolher opções diferentes, você pode forçar o **rpm** a ignorar esses padrões, mas isso é somente para especialistas. Caso contrário, você se arrisca a comprometer a integridade do sistema e, possivelmente, ameaça a capacidade de atualização do sistema.

As opções `-U` ou `--upgrade` e `-F` ou `--freshen` podem ser usadas para atualizar um pacote (por exemplo, **rpm -F** *pacote*`.rpm`). Esse comando remove os arquivos da versão antiga e instala os novos arquivos imediatamente. A diferença entre as duas versões é que o `-U` instala pacotes que não existiam no sistema anteriormente, mas `-F` atualiza somente pacotes previamente instalados. Durante a atualização, o **rpm** atualiza arquivos de configuração cuidadosamente com a seguinte estratégia:

- Se um arquivo de configuração não tiver sido modificado pelo administrador de sistema, o **rpm** instalará a nova versão do arquivo apropriado. O administrador de sistema não precisa adotar nenhuma ação.

- Se um arquivo de configuração tiver sido mudado pelo administrador do sistema antes da atualização, o **rpm** gravará o arquivo mudado com a extensão `.rpmorig` ou `.rpmsave` (arquivo de backup) e instalará a versão do novo pacote (mas somente se o arquivo instalado originalmente e a versão mais nova forem diferentes). Nesse caso, compare o arquivo de backup (`.rpmorig` ou `.rpmsave`) com o arquivo recém-instalado e faça novamente as modificações no novo arquivo. Depois, verifique se apagou todos os arquivos `.rpmorig` e `.rpmsave` para evitar problemas em atualizações futuras.

- Arquivos `.rpmnew` são exibidos se o arquivo de configuração já existir *e* se o rótulo `noreplace` tiver sido especificado no arquivo `.spec`.

Após uma atualização, os arquivos `.rpmsave` e `.rpmnew` devem ser removidos depois de comparados, para que não impeçam atualizações futuras. A extensão `.rpmorig` será atribuída se o arquivo não tiver sido previamente reconhecido pelo banco de dados RPM.

Caso contrário, o `.rpmsave` será usado. Em outras palavras, o `.rpmorig` resulta da atualização de um formato estranho ao RPM. `0 .rpmsave` resulta da atualização de um RPM mais antigo para um RPM mais novo. `0 .rpmnew` não revela se o administrador do sistema fez mudanças no arquivo de configuração. Uma lista destes arquivos está disponível em `/var/adm/rpmconfigcheck`. Alguns arquivos de configuração (como `/etc/httpd/httpd.conf`) não são sobregravados para permitir operação continuada.

O switch `-U` *não* é somente um equivalente para a desinstalação com a opção `-e` e a instalação com a opção `-i`. Use `-U` sempre que possível.

Para remover um pacote, digite **`rpm -e`** *`pacote`*. Este comando só apaga o pacote quando não há dependências não resolvidas. É teoricamente impossível apagar Tcl/Tk, por exemplo, enquanto outro aplicativo exigir sua existência. Mesmo nesse caso, o RPM pede ajuda do banco de dados. Se, por qualquer motivo, a exclusão for impossível (mesmo que não exista *nenhuma* dependência adicional), talvez seja útil reconstruir o banco de dados RPM usando a opção `--rebuilddb`.

7.2.3 Pacotes RPM Delta

Os pacotes RPM Delta possuem uma diferença entre uma versão nova e antiga de um pacote RPM. Aplicar um RPM delta a um RPM antigo resulta em um RPM completamente novo. Não é necessário ter uma cópia do RPM antigo, pois um RPM delta também pode funcionar com um RPM instalado. Os pacotes RPM delta têm tamanho ainda menor que os RPMs com patch, o que é uma vantagem durante a transferência de pacotes de atualização na Internet. A desvantagem é que operações de atualização que envolvem RPMs delta consomem consideravelmente mais ciclos de CPU do que as operações com RPMs com patch ou simples.

Os binários **`makedeltarpm`** e **`applydelta`** integram a suíte de RPM delta (pacote `deltarpm`) e ajudam na criação e aplicação de pacotes RPM delta. Com os seguintes comandos, crie um RPM delta chamado `new.delta.rpm`. O comando a seguir pressupõe que `old.rpm` e `new.rpm` estejam presentes:

```
makedeltarpm old.rpm new.rpm new.delta.rpm
```

Usando **`applydeltarpm`**, você poderá reconstruir o novo RPM do arquivo de sistema, se o pacote antigo já estiver instalado:

```
applydeltarpm new.delta.rpm new.rpm
```

Para derivá-lo do RPM antigo sem acessar o sistema de arquivos, use a opção `-r`:

```
applydeltarpm -r old.rpm new.delta.rpm new.rpm
```

Consulte `/usr/share/doc/packages/deltarpm/README` para obter os detalhes técnicos.

7.2.4 Consultas de RPM

Com a opção `-q`, o **`rpm`** inicia consultas, permitindo a inspeção de um arquivo RPM (adicionando-se a opção `-p`) e também a consulta ao banco de dados RPM de pacotes instalados. Vários switches estão disponíveis para especificar o tipo de informação necessária. Consulte a *Tabela 7.1, "Opções mais importantes de consulta de RPM"*.

TABELA 7.1 OPÇÕES MAIS IMPORTANTES DE CONSULTA DE RPM

`-i`	Informações de pacote
`-l`	Lista de arquivos
`-f ARQUIVO`	Consulte o pacote que contém o arquivo *`ARQUIVO`* (o caminho completo deve ser especificado com *`ARQUIVO`*)
`-s`	Lista de arquivos com informações de status (requer `-l`)
`-d`	Lista somente arquivos de documentação (requer `-l`)
`-c`	Lista somente arquivos de configuração (requer `-l`)
`--dump`	Lista de arquivos com detalhes completos (a ser usada com `-l`, `-c` ou `-d`)
`--provides`	Lista recursos do pacote que outro pacote pode solicitar com `--requires`
`--requires`, `-R`	Recursos exigidos pelo pacote
`--scripts`	Scripts de instalação (pré-instalação, pós-instalação, desinstalação)

Por exemplo, o comando **`rpm -q -i wget`** exibe as informações mostradas no *Exemplo 7.2, "rpm -q -i wget"*.

EXEMPLO 7.2 RPM -Q -I WGET

```
Name        : wget                          Relocations: (not relocatable)
Version     : 1.11.4                             Vendor: openSUSE
Release     : 1.70                           Build Date: Sat 01 Aug 2009 09:49:48
 CEST
Install Date: Thu 06 Aug 2009 14:53:24 CEST      Build Host: build18
Group       : Productivity/Networking/Web/Utilities   Source RPM:
 wget-1.11.4-1.70.src.rpm
Size        : 1525431                           License: GPL v3 or later
Signature   : RSA/8, Sat 01 Aug 2009 09:50:04 CEST, Key ID b88b2fd43dbdc284
Packager    : http://bugs.opensuse.org
URL         : http://www.gnu.org/software/wget/
Summary     : A Tool for Mirroring FTP and HTTP Servers
Description :
Wget enables you to retrieve WWW documents or FTP files from a server.
This can be done in script files or via the command line.
[...]
```

A opção `-f` funcionará somente se você especificar o nome e o caminho completos do arquivo. Insira quantos nomes de arquivo desejar. Por exemplo, o seguinte comando

```
rpm -q -f /bin/rpm /usr/bin/wget
```

resulta em:

```
rpm-4.8.0-4.3.x86_64
wget-1.11.4-11.18.x86_64
```

Se apenas parte do nome de arquivo for conhecida, use um script de shell conforme mostrado no *Exemplo 7.3, “Script para pesquisar pacotes”*. Passe o nome de arquivo parcial para o script mostrado como um parâmetro ao executá-lo.

EXEMPLO 7.3 SCRIPT PARA PESQUISAR PACOTES

```
#! /bin/sh
for i in $(rpm -q -a -l | grep $1); do
    echo "\"$i\" is in package:"
```

```
    rpm -q -f $i
    echo ""
done
```

O comando **rpm -q --changelog** *pacote* exibe uma lista detalhada com as informações de modificações sobre determinado pacote, classificadas por data.

Com a ajuda do banco de dados RPM instalado, é possível realizar verificações. Inicie as verificações com `-V` ou `--verify`. Com essa opção, o **rpm** mostra todos os arquivos em um pacote que foram modificados desde a instalação. O **rpm** usa oito símbolos de caracteres para fornecer algumas dicas sobre as seguintes mudanças:

TABELA 7.2 OPÇÕES DE VERIFICAÇÃO DO RPM

`5`	Resumo de verificação MD5
`S`	Tamanho do arquivo
`L`	Link simbólico
`T`	Tempo de modificação
`D`	Números de dispositivo principais e auxiliares
`U`	Proprietário
`C`	Grupo
`M`	Modo (tipo de arquivo e permissões)

No caso de arquivos de configuração, a letra `c` é impressa. Por exemplo, para modificações no pacote `/etc/wgetrc` (`wget`):

```
rpm -V wget
S.5....T c /etc/wgetrc
```

Os arquivos do banco de dados RPM são colocados em `/var/lib/rpm`. Se a partição `/usr` tiver o tamanho de 1 GB, esse banco de dados poderá ocupar praticamente 30 MB, especialmente após uma atualização completa. Se o banco de dados for maior do que o esperado, será útil reconstruir o banco de dados com a opção `--rebuilddb`. Antes disso, faça um backup do banco

de dados antigo. O script **cron** **cron.daily** faz cópias diárias do banco de dados (compactado com gzip) e as armazena em `/var/adm/backup/rpmdb`. O número de cópias é controlado pela variável `MAX_RPMDB_BACKUPS` (padrão: `5`) em `/etc/sysconfig/backup`. O tamanho de um único backup é de aproximadamente 1 MB para 1 GB em `/usr`.

7.2.5 Instalando e compilando pacotes de fonte

Todos os pacotes de fonte têm a extensão `.src.rpm` (RPM de fonte).

Nota: Pacotes de fontes instalados

Pacotes de fonte podem ser copiados da mídia de instalação para o disco rígido e descompactados com o YaST. Porém, eles não são marcados como instalados (`[i]`) no gerenciador de pacotes. Isso ocorre porque os pacotes de fontes não são inseridos no banco de dados RPM. Somente o software do sistema operacional *instalado* está listado no banco de dados RPM. Quando você "instalar" um pacote de fontes, somente o código-fonte será adicionado ao sistema.

Os diretórios a seguir devem estar disponíveis para **rpm** e **rpmbuild** em `/usr/src/packages` (a menos que você tenha especificado configurações personalizadas em um arquivo como `/etc/rpmrc`):

`SOURCES`
: para as fontes originais (arquivos `.tar.bz2` ou `.tar.gz` etc.) e para ajustes específicos de distribuição (geralmente arquivos `.diff` ou `.patch`)

`SPECS`
: para os arquivos `.spec`, similares a um metaMakefile, que controla o processo de *construção*

`BUILD`
: diretório em que todas as fontes são descompactadas, corrigidas e compiladas

`RPMS`
: local em que os pacotes binários concluídos são armazenados

`SRPMS`
: local em que estão os RPMs de fonte

Quando você instala um pacote de fontes com o YaST, todos os componentes necessários são instalados em `/usr/src/packages`: as fontes e os ajustes em `SOURCES` e o arquivo `.spec` relevante em `SPECS`.

Atenção: Integridade do Sistema

Não faça experiências com os componentes do sistema (`glibc`, `rpm`, etc.), pois isso arrisca a estabilidade do sistema.

O exemplo a seguir usa o pacote `wget.src.rpm.` Após instalar o pacote de origem, você deverá ter arquivos semelhantes aos da seguinte lista:

```
/usr/src/packages/SOURCES/wget-1.11.4.tar.bz2
/usr/src/packages/SOURCES/wgetrc.patch
/usr/src/packages/SPECS/wget.spec
```

`rpmbuild -b` *`X`* **`/usr/src/packages/SPECS/wget.spec`** inicia a compilação. *`X`* é um curinga para vários estágios do processo de construção (consulte a saída de `--help` ou a documentação do RPM para obter os detalhes). Veja a seguir uma breve explicação:

`-bp`

Preparar as fontes em `/usr/src/packages/BUILD`: descompactar e corrigir.

`-bc`

Faz o mesmo que `-bp`, mas com compilação adicional.

`-bi`

Faz o mesmo que `-bp`, mas com a instalação adicional do software criado. Cuidado: se o pacote não aceitar o recurso BuildRoot, talvez você sobregrave os arquivos de configuração.

`-bb`

Faz o mesmo que `-bi`, mas com a criação adicional do pacote binário. Se a compilação tiver sido bem-sucedida, o binário deverá estar em `/usr/src/packages/RPMS`.

`-ba`

Faz o mesmo que `-bb`, mas com a criação adicional do RPM de fonte. Se a compilação tiver sido bem-sucedida, o binário deverá estar em `/usr/src/packages/SRPMS`.

`--short-circuit`

Ignora algumas etapas.

O RPM binário criado agora pode ser instalado com **`rpm -i`** ou, de preferência, com **`rpm -U`**. A instalação com **`rpm`** faz com que ele apareça no banco de dados RPM.

7.2.6 Compilando pacotes RPM com build

O perigo de vários pacotes é que arquivos indesejados são adicionados ao sistema em execução durante o processo de construção. Para evitar isso, use `build`, que cria um ambiente definido para construção do pacote. Para estabelecer esse ambiente chroot, o script **`build`** deve ser fornecido com uma árvore de pacote completa. Essa árvore pode ser disponibilizada no disco rígido, por meio do NFS ou DVD. Defina a posição com **`build --rpms`** *`diretório`*. Diferentemente do **`rpm`**, o comando **`build`** procura o arquivo `.spec` no diretório de fontes. Para construir o `wget` (como no exemplo acima) com o DVD montado no sistema em `/media/dvd`, use o seguinte comando como `root`:

```
cd /usr/src/packages/SOURCES/
mv ../SPECS/wget.spec .
build --rpms /media/dvd/suse/ wget.spec
```

Depois disso, um ambiente mínimo é estabelecido em `/var/tmp/build-root`. O pacote é criado nesse ambiente. Após a conclusão, os pacotes resultantes estarão localizados em `/var/tmp/build-root/usr/src/packages/RPMS`.

O script **`build`** oferece várias opções adicionais. Por exemplo, fazer com que o script prefira seus próprios RPMs, omitir a inicialização do ambiente de construção ou limitar o comando **`rpm`** a um dos estágios mencionados acima. Acesse informações adicionais com **`build --help`** e a leitura da página de manual **`build`**.

7.2.7 Ferramentas para arquivos RPM e banco de dados RPM

O Midnight Commander (**`mc`**) pode exibir o conteúdo de arquivos RPM e copiar partes deles. Ele representa arquivos como sistemas de arquivos virtuais, oferecendo todas as opções de menu usuais do Midnight Commander. Exiba o `HEADER` com F3. Exiba a estrutura de arquivos com as teclas de cursor e Enter. Copie componentes de arquivos com F5.

Um gerenciador de pacote completo está disponível como um módulo do YaST. Para obter os detalhes, consulte o *Book "*Deployment Guide*" 6 "Installing or Removing Software"*.

8 Bash e scripts Bash

Atualmente, muitas pessoas usam computadores com uma GUI (interface gráfica do usuário) como o GNOME. Embora ela ofereça muitos recursos, seu uso é limitado quando se trata de execução de tarefas automatizadas. Shells são bons aliados das interfaces gráficas, por isso este capítulo apresenta uma visão geral de alguns aspectos dos shells, neste caso, o Bash.

8.1 O que é "o shell"?

Tradicionalmente, *o* shell é o Bash (Bourne again Shell). Quando este capítulo menciona "o shell", ele se refere ao Bash. Na verdade, há mais shells disponíveis além do Bash (ash, csh, ksh, zsh, etc.), cada um deles empregando recursos e características diferentes. Se você precisar de mais informações sobre outros shells, pesquise por *shell* no YaST.

8.1.1 Conhecendo os arquivos de configuração do Bash

Um shell pode ser acionado como:

1. **Shell de login interativo.** Esse tipo é usado para efetuar login em uma máquina, chamando o Bash com a opção `--login`, ou para efetuar login em uma máquina remota com SSH.
2. **Shell interativo "comum".** Normalmente esse é o caso quando se inicia o xterm, o konsole, o gnome-terminal ou ferramentas semelhantes.
3. **Shell não interativo.** Usado para chamar um script de shell na linha de comando.

Dependendo do tipo de shell usado, variam os arquivos de configuração lidos. As tabelas seguintes mostram os arquivos de configuração de shell de login e sem login.

TABELA 8.1 ARQUIVOS DE CONFIGURAÇÃO DO BASH PARA SHELLS DE LOGIN

Arquivo	Descrição
`/etc/profile`	Não modifique esse arquivo, senão as suas modificações poderão ser destruídas durante a próxima atualização!

Arquivo	Descrição
`/etc/profile.local`	Use esse arquivos se for estender `/etc/profile`
`/etc/profile.d/`	Contém arquivos de configuração de programas específicos para todo o sistema
`~/.profile`	Insira aqui a configuração específica de usuário para os shells de login

TABELA 8.2 ARQUIVOS DE CONFIGURAÇÃO DO BASH PARA SHELLS SEM LOGIN

`/etc/bash.bashrc`	Não modifique esse arquivo, senão as suas modificações poderão ser destruídas durante a próxima atualização!
`/etc/bash.bashrc.local`	Use esse arquivo para inserir suas modificações apenas do Bash em todo o sistema
`~/.bashrc`	Insira aqui a configuração específica de usuário

Além desses, o Bash usa mais outros arquivos:

TABELA 8.3 ARQUIVOS ESPECIAIS DO BASH

Arquivo	Descrição
`~/.bash_history`	Contém uma lista de todos os comandos que você digitou
`~/.bash_logout`	Executado durante o logout

8.1.2 Estrutura de diretórios

A tabela a seguir fornece uma breve visão geral dos mais importantes diretórios de nível superior encontrados em um sistema Linux. Informações mais detalhadas sobre os diretórios e subdiretórios importantes são encontradas na lista a seguir.

TABELA 8.4 VISÃO GERAL DE UMA ÁRVORE DE DIRETÓRIO PADRÃO

Diretório	Conteúdo
`/`	Diretório raiz: o ponto de partida da árvore do diretório.
`/bin`	Arquivos binários essenciais, como comandos necessários pelo administrador do sistema e por usuários comuns. Geralmente contém os shells, como o Bash.
`/boot`	Arquivos estáticos do carregador de boot.
`/dev`	Arquivos necessários para acessar dispositivos específicos de host.
`/etc`	Arquivos de configuração do sistema específicos de host.
`/home`	Contém os diretórios pessoais de todos os usuários que possuem conta no sistema. Porém, o diretório pessoal do `root` não está em `/home`, mas sim em `/root`.
`/lib`	Bibliotecas compartilhadas e módulos de kernel essenciais.
`/media`	Pontos de montagem de mídia removível.
`/mnt`	Ponto de montagem para montar temporariamente um sistema de arquivos.
`/opt`	Pacotes de aplicativos complementares.
`/root`	Diretório pessoal do superusuário `root`.
`/sbin`	Binários essenciais do sistema.
`/srv`	Dados de serviços fornecidos pelo sistema.
`/tmp`	Arquivos temporários.
`/usr`	Contém os dados básicos do shell que podem ser usados pelo root e por outros usuários. Esses comandos incluem `ls`, `mkdir`, `cp`, `mv`, `rm` e `rmdir`. O `/bin` também contém o Bash, o shell padrão do SUSE Linux Enterprise Desktop.
`/var`	Dados variáveis, como arquivos de registro.
`/windows`	Disponível apenas se você tiver o Microsoft Windows* e o Linux instalados no sistema. Contém os dados do Windows.

A lista a seguir fornece informações mais detalhadas e alguns exemplos de arquivos e subdiretórios encontrados nos diretórios da hierarquia secundária com dados apenas leitura.

/bin

`/boot`

Contém dados necessários para inicializar, como o carregador de boot, o kernel e outros dados usados para que o kernel possa executar programas em modo de usuário.

`/dev`

Contém arquivos de dispositivos que representam componentes de hardware.

`/etc`

Contém arquivos de configuração local que controlam a operação de programas como o Sistema X Window. O subdiretório `/etc/init.d` contém scripts init LSB que podem ser executados durante o processo de boot.

`/home/`*`nome_do_usuário`*

Contém os dados privados de todos os usuários que possuem uma conta no sistema. Os arquivos localizados aqui apenas podem ser modificados por seu proprietário ou pelo administrador do sistema. Por padrão, o diretório de e-mail e a configuração de área de trabalho pessoal estão localizados aqui, na forma de arquivos e diretórios ocultos, como `.gconf/` e `.config`.

Nota: diretório pessoal em um ambiente de rede

Se você estiver trabalhando em um ambiente de rede, seu diretório pessoal poderá ser mapeado para um diretório no sistema de arquivos diferente de `/home`.

`/lib`

Contém as bibliotecas compartilhadas essenciais necessárias para inicializar o sistema e executar os comandos no sistema de arquivos raiz. O equivalente no Windows para as bibliotecas compartilhadas são os arquivos DLL.

`/media`

Contém pontos de montagem para mídia removível, como CD-ROMs, discos flash e câmeras digitais (se usarem USB). `/media` geralmente mantém qualquer tipo de unidade, exceto o disco rígido do sistema. Assim que a mídia removível for inserida ou conectada no sistema e estiver montada, você poderá acessá-la a partir daqui.

`/mnt`

O diretório fornece um ponto de montagem para um sistema de arquivos montado temporariamente. O `root` pode montar sistemas de arquivos aqui.

`/opt`

Reservado para a instalação de software de terceiros. Software opcional e pacotes de programas complementares maiores são encontrados aqui.

`/root`

Diretório pessoal do usuário `root`. Os dados pessoais do `root` estão localizados aqui.

`/run`

Um diretório tmpfs usado pelo `systemd` e por vários componentes.

`/sbin`

Como indicado pelo `s`, esse diretório contém utilitários do superusuário. `/sbin` contém os binários essenciais para boot, restauração e recuperação do sistema, além dos binários em `/bin`.

`/srv`

Contém dados de serviços fornecidos pelo sistema, como FTP e HTTP.

`/tmp`

Esse diretório é usado por programas que exigem o armazenamento temporário dos arquivos.

Importante: Limpando `/tmp` em tempo de boot

Os dados armazenados em `/tmp` podem não existir após uma reinicialização do sistema. Depende, por exemplo, das configurações em `/etc/sysconfig/cron`.

`/usr`

O `/usr` não tem relação com os usuários, mas se trata do acrônimo de Unix system resources (recursos do sistema Unix). Os dados em `/usr` são estáticos e apenas leitura, podendo ser compartilhados entre vários hosts compatíveis com FHS (`Filesystem Hierarchy Standard` – Padrão da Hierarquia do Sistema de Arquivos). Este diretório contém todos os programas de aplicativo, incluindo as áreas de trabalho gráficas, como o GNOME, e estabelece uma hierarquia secundária no sistema de arquivos. `/usr` contém alguns subdiretórios como `/usr/bin`, `/usr/sbin`, `/usr/local` e `/usr/share/doc`.

`/usr/bin`

Contém programas geralmente acessíveis.

`/usr/bin`

Contém programas reservados ao administrador do sistema, como as funções de reparo.

`/usr/local`

Nesse diretório, o administrador do sistema pode instalar extensões locais e independentes de distribuição.

`/usr/share/doc`

Contém vários arquivos de documentação e as notas de versão do sistema. No subdiretório `manual`, você encontra uma versão online deste manual. Se houver mais de um idioma instalado, esse diretório poderá conter versões dos manuais em idiomas diferentes.

Em `packages`, você encontra a documentação incluída nos pacotes de software instalados no sistema. Para cada pacote, é criado um subdiretório `/usr/share/doc/packages/`*`nome_do_pacote`*, geralmente contendo arquivos README do pacote e, por vezes, exemplos, arquivos de configuração ou scripts adicionais.

Se houver HOWTOs instalados no sistema, `/usr/share/doc` também conterá o subdiretório `howto`, com documentação adicional sobre muitas tarefas relacionadas a configuração e operação do software Linux.

`/var`

Ao passo que `/usr` contém dados estáticos apenas leitura, `/var` destina-se aos dados gravados durante a operação do sistema, portanto variáveis, como arquivos de registro ou de spool. Para obter uma visão geral dos arquivos de registro mais importantes que estão em `/var/log/`, consulte a *Tabela 30.1, "Arquivos de registro"*.

`/windows`

Disponível apenas se você tiver o Microsoft Windows e o Linux instalados no sistema. Contém os dados do Windows disponíveis na partição Windows do sistema. A sua capacidade de editar dados nesse diretório depende do sistema de arquivos usado pelas partições Windows. No caso do FAT32, você pode abrir e editar os arquivos desse diretório. Para NTFS, o SUSE Linux Enterprise Desktop também oferece suporte a acesso de gravação. No entanto, o driver para o sistema de arquivos NTFS-3g possui funcionalidade limitada.

8.2 Gravando scripts shell

Scripts shell são convenientes para todos os tipos de tarefas: coleta de dados, pesquisa por uma palavra ou frase em um texto e muitas outras coisas úteis. O exemplo seguinte mostra um pequeno script shell que imprime um texto:

EXEMPLO 8.1 UM SCRIPT SHELL QUE IMPRIME UM TEXTO

```
#!/bin/sh ❶
# Output the following line: ❷
echo "Hello World" ❸
```

❶ A primeira linha começa com os caracteres *Shebang* (`#!`), indicando que o arquivo é um script. O script é executado pelo interpretador especificado após o Shebang, neste caso, **`/bin/sh`**.

❷ A segunda linha é um comentário que começa com o sinal de hash. Ele é recomendado para inserir comentário em linhas cuja função é difícil de lembrar.

❸ A terceira linha usa o comando interno **`echo`** para imprimir o texto correspondente.

Antes de executar esse script, você precisa de alguns pré-requisitos:

1. Todo script deve conter uma linha Shebang (como foi o caso do nosso exemplo acima). Se um script não tiver essa linha, você deverá chamar o interpretador manualmente.
2. Grave o script no lugar desejado. Contudo, convém gravá-lo em um diretório onde o shell possa encontrá-lo. O caminho de pesquisa em um shell é determinado pela variável de ambiente `PATH`. Um usuário normal geralmente não tem acesso de gravação em `/usr/bin`. Por essa razão, recomenda-se gravar seus scripts no diretório `~/bin/` dos usuários. O exemplo acima leva o nome `hello.sh`.
3. O script requer permissões de executável. Defina as permissões com o seguinte comando:

   ```
   chmod +x ~/bin/hello.sh
   ```

Se você atendeu a todos os pré-requisitos acima, poderá executar o script das seguintes maneiras:

1. **Como caminho absoluto.** O script pode ser executado em um caminho absoluto. No nosso caso, ele é **`~/bin/hello.sh`**.
2. **Em todos os lugares.** Se a variável de ambiente `PATH` incluir o diretório no qual o script está localizado, você poderá executar o script usando o comando **`hello.sh`**.

8.3 Redirecionando eventos de comando

Cada comando pode usar três canais, seja para entrada ou para saída:

- **Saída padrão.** Esse é o canal de saída padrão. Sempre que um comando imprime algo, ele usa o canal de saída padrão.
- **Entrada padrão.** Se um comando precisar da entrada dos usuários ou de outros comandos, ele usará esse canal.
- **Erro padrão.** Os comandos usam esse canal para gerar relatórios de erros.

Para redirecionar os canais, as possibilidades são as seguintes:

`Comando > Arquivo`

Grava a saída do comando em um arquivo, apagando um arquivo existente. Por exemplo, o comando **`ls`** grava sua saída no arquivo `listing.txt`:

```
ls > listing.txt
```

`Comando >> Arquivo`

Anexa a saída do comando a um arquivo. Por exemplo, o comando **`ls`** anexa sua saída ao arquivo `listing.txt`:

```
ls >> listing.txt
```

`Comando < Arquivo`

Lê o arquivo como entrada do comando em questão. Por exemplo, o comando **`read`** extrai o conteúdo do arquivo para a variável:

```
read a < foo
```

`Comando1 | Comando2`

Redireciona a saída do comando à esquerda como entrada para o comando à direita. Por exemplo, o comando **`cat`** gera a saída do conteúdo do arquivo `/proc/cpuinfo`. Essa saída é usada por **`grep`** para filtrar apenas as linhas que contêm `cpu`:

```
cat /proc/cpuinfo | grep cpu
```

Cada canal possui um *descritor de arquivo*: 0 (zero) para entrada padrão, 1 para saída padrão e 2 para erro padrão. É permitido inserir esse descritor de arquivo antes de um caractere `<` ou `>`. Por exemplo, a linha a seguir procura por um arquivo que começa com `foo`, mas suprime seus erros redirecionando-o para `/dev/null`:

```
find / -name "foo*" 2>/dev/null
```

8.4 Usando álias

Um álias é uma definição de atalho de um ou mais comandos. A sintaxe de um álias é a seguinte:

```
alias NAME=DEFINITION
```

Por exemplo, a linha a seguir define um álias **`lt`** que gera uma listagem extensa (opção `-l`), classifica-a por horário de modificação (`-t`) e imprime-a em ordem inversa ao classificar (`-r`):

```
alias lt='ls -ltr'
```

Para ver todas as definições de álias, use **`alias`** Remova o seu álias com **`unalias`** e o nome de álias correspondente.

8.5 Usando variáveis no Bash

Uma variável de shell pode ser global ou local. Variáveis globais, ou de ambiente, podem ser acessadas em todos os shells. As variáveis locais, ao contrário, são visíveis apenas no shell atual.

Para ver todas as variáveis de ambiente, use o comando **`printenv`**. Se for preciso saber o valor de uma variável, insira o nome da variável como argumento:

```
printenv PATH
```

Uma variável, seja ela global ou local, também pode ser visualizada com **`echo`**:

```
echo $PATH
```

Para definir uma variável local, use um nome de variável, seguido pelo sinal de igual, seguido pelo valor:

```
PROJECT="SLED"
```

Não insira espaços antes e depois do sinal de igual, senão você obterá um erro. Para definir uma variável de ambiente, use **`export`**:

```
export NAME="tux"
```

Para remover uma variável, use **`unset`**:

```
unset NAME
```

A tabela a seguir contém algumas variáveis de ambiente comuns que podem ser usadas nos seus scripts shell:

TABELA 8.5 VARIÁVEIS DE AMBIENTE ÚTEIS

`HOME`	diretório pessoal do usuário atual
`HOST`	nome do host atual
`LANG`	quando uma ferramenta é localizada, ela usa o idioma dessa variável de ambiente. Também é possível definir o idioma inglês como `C`
`PATH`	caminho de pesquisa do shell, uma lista de diretórios separados por dois-pontos
`PS1`	especifica o prompt normal impresso antes de cada comando
`PS2`	especifica o prompt secundário impresso quando você executa um comando em várias linhas
`PWD`	diretório de trabalho atual
`USER`	usuário atual

8.5.1 Usando variáveis de argumento

Por exemplo, se você tiver o script **`foo.sh`**, poderá executá-lo desta maneira:

```
foo.sh "Tux Penguin" 2000
```

Para acessar todos os argumentos que são passados ao seu script, você precisa de parâmetros de posição. Isto é, `$1` para o primeiro argumento, `$2` para o segundo e assim sucessivamente. É possível usar até nove parâmetros. Para obter o nome do script, use `$0`.

O script **`foo.sh`** a seguir imprime todos os argumentos de 1 a 4:

```
#!/bin/sh
echo \"$1\" \"$2\" \"$3\" \"$4\"
```

Se você executar esse script com os argumentos acima, obterá:

```
"Tux Penguin" "2000" "" ""
```

8.5.2 Usando substituição de variável

As substituições de variáveis aplicam um padrão ao conteúdo de uma variável, seja da esquerda ou da esquerda. A lista a seguir contém as formas de sintaxe possíveis:

`${VAR#padrão}`
: remove a correspondência mais curta possível da esquerda:

```
file=/home/tux/book/book.tar.bz2
echo ${file#*/}
home/tux/book/book.tar.bz2
```

`${VAR##padrão}`
: remove a correspondência mais longa possível da esquerda:

```
file=/home/tux/book/book.tar.bz2
echo ${file##*/}
book.tar.bz2
```

`${VAR%padrão}`

remove a correspondência mais curta possível da direita:

```
file=/home/tux/book/book.tar.bz2
echo ${file%.*}
/home/tux/book/book.tar
```

`${VAR%%padrão}`

remove a correspondência mais longa possível da direita:

```
file=/home/tux/book/book.tar.bz2
echo ${file%%.*}
/home/tux/book/book
```

`${VAR/padrão_1/padrão_2}`

substitui o conteúdo de *`VAR`* do *`padrão_1`* pelo do *`padrão_2`*:

```
file=/home/tux/book/book.tar.bz2
echo ${file/tux/wilber}
/home/wilber/book/book.tar.bz2
```

8.6 Agrupando e combinando comandos

Os shells permitem concatenar e agrupar comandos para uma execução condicional. Cada comando retorna um código de saída que determina o sucesso ou a falha de sua operação. Se o código for 0 (zero), significa que o comando obteve sucesso. Todos os outros códigos significam erro específico do comando.

A lista a seguir mostra como os comandos podem ser agrupados:

`Comando1 ; Comando2`

executa os comandos em sequência. O código de saída não é verificado. A linha a seguir exibe o conteúdo do arquivo com **`cat`** e depois imprime suas propriedades com **`ls`**, independentemente dos códigos de erro:

```
cat filelist.txt ; ls -l filelist.txt
```

`Comando1 && Comando2`

executa o comando à direita quando o comando à esquerda for bem-sucedido (E lógico). A linha a seguir exibe o conteúdo do arquivo e imprime suas propriedades apenas quando o comando anterior obtiver sucesso (compare com a entrada anterior nesta lista):

```
cat filelist.txt && ls -l filelist.txt
```

`Comando1 || Comando2`

executa o comando à direita quando o comando da esquerda falhar (OU lógico). A linha a seguir cria um diretório em `/home/wilber/bar` apenas quando a criação do diretório em `/home/tux/foo` falhar:

```
mkdir /home/tux/foo || mkdir /home/wilber/bar
```

`nome_da_função(){ ... }`

cria uma função shell. Você pode usar os parâmetros de posição para acessar seus argumentos. A linha a seguir define a função `hello` para imprimir uma mensagem curta:

```
hello() { echo "Hello $1"; }
```

Você pode chamar essa função assim:

```
hello Tux
```

que imprimirá:

```
Hello Tux
```

8.7 Trabalhando com construções de fluxo comuns

Para controlar o fluxo do seu script, um shell possui as construções **`while`**, **`if`**, **`for`** e **`case`**.

8.7.1 Comando de controle if

O comando **`if`** é usado para verificar expressões. Por exemplo, o código a seguir testa se o usuário atual é Tux:

```
if test $USER = "tux"; then
  echo "Hello Tux."
else
  echo "You are not Tux."
fi
```

A expressão de teste pode ser tão complexa ou simples quanto possível. a expressão a seguir verifica se o arquivo `foo.txt` existe:

```
if test -e /tmp/foo.txt ; then
  echo "Found foo.txt"
fi
```

A expressão de teste também pode ser abreviada entre colchetes:

```
if [ -e /tmp/foo.txt ] ; then
  echo "Found foo.txt"
fi
```

Outras expressões úteis estão disponíveis em http://www.cyberciti.biz/nixcraft/linux/docs/uniqlinuxfeatures/lsst/ch03sec02.html.

8.7.2 Criando loops com o comando for

O loop **`for`** permite executar comandos para uma lista de entradas. Por exemplo, o código a seguir imprime algumas informações sobre arquivos PNG no diretório atual:

```
for i in *.png; do
 ls -l $i
done
```

8.8 Para obter mais informações

Informações importantes sobre o Bash são fornecidas nas páginas de manual **`man bash`**. Mais informações sobre este tópico estão disponíveis na lista a seguir:

- http://tldp.org/LDP/Bash-Beginners-Guide/html/index.html — Bash Guide for Beginners (Guia do Bash para Iniciantes)
- http://tldp.org/HOWTO/Bash-Prog-Intro-HOWTO.html — BASH Programming - Introduction HOW-TO (COMO FAZER Programação de Bash: Introdução)
- http://tldp.org/LDP/abs/html/index.html — Advanced Bash-Scripting Guide (Guia Avançado de Criação de Scripts Bash)
- http://www.grymoire.com/Unix/Sh.html — Sh - the Bourne Shell (Sh: o Bourne Shell)

II Sistema

9 Aplicativos de 32 bits e 64 bits em um ambiente de sistema de 64 bits 117

10 Inicializando um sistema Linux 121

11 O daemon `systemd` 126

12 **`journalctl`**: consultar o diário do `systemd` 150

13 O carregador de boot GRUB 2 158

14 UEFI (Unified Extensible Firmware Interface) 179

15 Recursos especiais do sistema 188

16 Operação da impressora 202

17 Gerenciamento dinâmico de dispositivos do Kernel com udev 218

18 O sistema X Window 232

19 Acessando sistemas de arquivos com o FUSE 247

9 Aplicativos de 32 bits e 64 bits em um ambiente de sistema de 64 bits

O SUSE® Linux Enterprise Desktop está disponível para plataformas de 64 bits. Isso não significa necessariamente que todos os aplicativos incluídos tenham sido transpostos para plataformas de 64 bits. O SUSE Linux Enterprise Desktop suporta o uso de aplicativos de 32 bits em um ambiente de sistema de 64 bits. Este capítulo apresenta uma breve visão geral de como este suporte é implementado em plataformas de 64 bits do SUSE Linux Enterprise Desktop. Ele explica como aplicativos de 32 bits são executados (suporte do tempo de execução) e como aplicativos de 32 bits devem ser compilados para que possam ser executados em ambientes de sistema de 32 bits e 64 bits. Além disso, você encontrará informações sobre a API do kernel e uma explicação sobre como os aplicativos de 32 bits podem ser executados em um kernel de 64 bits.

O SUSE Linux Enterprise Desktop para as plataformas de 64 bits amd64 e Intel 64 foi desenvolvido para que os aplicativos de 32 bits existentes sejam executados no ambiente de 64 bits “out-of-the-box.” Este suporte significa que você pode continuar a usar os aplicativos de 32 bits de sua preferência sem esperar que uma porta de 64 bits correspondente se torne disponível.

9.1 Suporte ao tempo de execução

Importante: conflitos entre versões de aplicativos

Se um aplicativo estiver disponível para ambientes de 32 bits e de 64 bits, a instalação paralela das duas versões provavelmente resultará em problemas. Em tais casos, opte pela instalação e pelo uso de uma das duas versões.

Uma exceção a essa regra é o PAM (módulo de autenticação conectável). O SUSE Linux Enterprise Desktop usa o PAM no processo de autenticação como uma camada mediadora entre o usuário e o aplicativo. Em um sistema operacional de 64 bits que também executa aplicativos de 32 bits, é necessário sempre instalar as duas versões de um módulo PAM.

Para que os aplicativos sejam executados corretamente, cada um deles requer uma variedade de bibliotecas. Infelizmente, os nomes das versões de 32 bits e 64 bits das bibliotecas são idênticos. Eles devem ser diferenciados uns dos outros de outra forma.

Para obter compatibilidade com a versão de 32 bits, as bibliotecas são armazenadas no mesmo local no sistema e no ambiente de 32 bits. A versão de 32 bits de `libc.so.6` está localizada em `/lib/libc.so.6` nos ambientes de 32 bits e 64 bits.

Todos os arquivos de objetos e todas as bibliotecas de 64 bits estão localizados em diretórios denominados `lib64`. Os arquivos de objeto de 64 bits, que normalmente são encontrados em `/lib` e em `/usr/lib`, agora estão em `/lib64` e em `/usr/lib64`. Isso significa que há espaço para as bibliotecas de 32 bits em `/lib` e em `/usr/lib`, permitindo que o nome de arquivo de ambas as versões permaneça inalterado.

Os subdiretórios dos diretórios `/lib` de 32 bits com conteúdo de dados que não depende do tamanho do texto não são movidos. Este esquema está em conformidade com a LSB (Linux Standards Base — Base de Padrões Linux) e com o FHS (File System Hierarchy Standard — Padrão de Hierarquia de Sistema de Arquivos).

9.2 Desenvolvimento de software

Uma cadeia de ferramentas de desenvolvimento biarch permite a geração de objetos de 32 bits e 64 bits. O padrão é compilar objetos de 64 bits. É possível gerar objetos de 32 bits usando sinalizadores especiais. Para GCC, o sinalizador especial é `-m32`.

Todos os arquivos de cabeçalho devem ser escritos em um formato independente de arquitetura. As bibliotecas de 32 bits e 64 bits instaladas devem ter uma API (application programming interface — interface de programação de aplicativo) que corresponda aos arquivos de cabeçalho instalados. O ambiente normal do SUSE Linux Enterprise Desktop foi desenvolvido de acordo com este princípio. No caso de bibliotecas atualizadas manualmente, solucione esses problemas por conta própria.

9.3 Compilação de software em plataformas biarch

Para desenvolver binários para outra arquitetura em uma arquitetura biarch, as respectivas bibliotecas da segunda arquitetura devem ser instaladas adicionalmente. Esses pacotes são chamados de `rpmname-32bit`. Você também precisará dos respectivos cabeçalhos e bibliotecas dos pacotes `rpmname-devel` e das bibliotecas de desenvolvimento para a segunda arquitetura de `rpmname-devel-32bit`.

A maioria dos programas de código-fonte aberto usa uma configuração de programa baseada em **autoconf**. Para usar o **autoconf** com o objetivo de configurar um programa para a segunda arquitetura, sobregrave as configurações do compilador normal e do linker de **autoconf** executando o script **configure** com variáveis de ambiente adicionais.

O exemplo a seguir refere-se a um sistema x86_64 com x86 como a segunda arquitetura.

1. Use o compilador de 32 bits:

```
CC="gcc -m32"
```

2. Instrua o linker a processar objetos de 32 bits (use sempre **gcc** como o front end do linker):

```
LD="gcc -m32"
```

3. Defina o assembler para gerar objetos de 32 bits:

```
AS="gcc -c -m32"
```

4. Especifique flags do linker, como o local das bibliotecas de 32 bits, por exemplo:

```
LDFLAGS="-L/usr/lib"
```

5. Especifique o local das bibliotecas de código objeto de 32 bits:

```
--libdir=/usr/lib
```

6. Especifique o local das bibliotecas X de 32 bits:

```
--x-libraries=/usr/lib
```

Nem todas essas variáveis são necessárias para todos os programas. Adapte-as para o respectivo programa.

```
CC="gcc -m32"
LDFLAGS="-L/usr/lib;"
./configure --prefix=/usr --libdir=/usr/lib --x-libraries=/usr/lib
make
make install
```

9.4 Especificações do kernel

Os kernels de 64 bits para o x86_64 oferecem uma ABI (interface binária de aplicativo) para kernel de 64 bits e de 32 bits. A de 64 bits é idêntica à ABI do kernel de 32 bits correspondente. Isso significa que o aplicativo de 32 bits pode se comunicar com o kernel de 64 bits da mesma forma que com o kernel de 32 bits.

A emulação de 32 bits de chamadas do sistema para um kernel de 64 bits não suporta todas as APIs usadas pelos programas do sistema. Isso depende da plataforma. Por isso, alguns poucos aplicativos, como o **`lspci`**, precisam ser compilados..

Um kernel de 64 bits só pode carregar módulos de kernel de 64 bits especificamente compilados para esse kernel. Não é possível usar módulos de kernel de 32 bits.

Dica: Módulos carregáveis pelo Kernel

Alguns aplicativos requerem módulos separados carregáveis pelo kernel. Se você pretende usar um aplicativo de 32 bits desse tipo em um ambiente de sistema de 64 bits, entre em contato com o provedor do aplicativo e do SUSE para verificar se a versão de 64 bits do módulo carregável pelo kernel e a versão compilada de 32 bits da API do kernel estão disponíveis para esse módulo.

10 Inicializando um sistema Linux

A inicialização de um sistema Linux envolve componentes e tarefas diferentes. O próprio hardware é inicializado pelo BIOS ou pela UEFI, que inicia o Kernel por meio de um carregador de boot. A partir deste ponto, o processo de boot é completamente controlado pelo sistema operacional e administrado pelo `systemd`. O `systemd` oferece um conjunto de "destinos" que inicializa configurações para uso diário, manutenção ou emergências.

10.1 Processo de boot do Linux

O processo de boot do Linux consiste em vários estágios, cada um deles representado por um componente diferente. A lista a seguir resume o processo de boot e apresenta todos os principais componentes envolvidos:

1. **BIOS/UEFI.** Após ligar o computador, o BIOS ou a UEFI inicializa a tela e o teclado e testa a memória principal. Até esse estágio, a máquina não acessa nenhuma mídia de armazenamento em massa. Em seguida, as informações sobre a data e o horário atuais e sobre os periféricos mais importantes são carregadas dos valores do CMOS. Quando o primeiro disco rígido e sua geometria são reconhecidos, o controle do sistema passa do BIOS para o carregador de boot. Se o BIOS oferecer suporte à inicialização pela rede, também será possível configurar um servidor de inicialização que ofereça o carregador de boot. Em sistemas x86_64, a inicialização PXE é necessária. Outras arquiteturas normalmente usam o protocolo BOOTP para obter o carregador de boot.

2. **Carregador de boot.** O primeiro setor de dados físico de 512 bytes do primeiro disco rígido é carregado na memória principal e o *carregador de boot* existente no início desse setor assume o controle. Os comandos executados pelo carregador de boot determinam a parte restante do processo de boot. Desse modo, os primeiros 512 bytes do primeiro disco rígido são chamados de MBR *(Master Boot Record)*. O carregador de boot passa o controle para o sistema operacional real, neste caso, o Kernel do Linux. Mais informações sobre o GRUB 2, o carregador de boot do Linux, podem ser encontradas no *Capítulo 13, O carregador de boot GRUB 2*. Para uma inicialização pela rede, o BIOS age como o carregador de boot. Ele obtém a imagem do servidor de boot e inicia o sistema. Isso é totalmente independente dos discos rígidos locais.

3. **Kernel e `initramfs`.** Para passar pelo controle do sistema, o carregador de boot carrega na memória o kernel e um sistema de arquivos inicial baseado em RAM (`initramfs`). O conteúdo do `initramfs` pode ser usado diretamente pelo Kernel. O `initramfs` contém um pequeno executável chamado `init` que faz a montagem do sistema de arquivos raiz real. Se forem necessários drivers de hardware especiais para acessar o armazenamento em massa, eles deverão estar em `initramfs`. Para obter mais informações sobre o `initramfs`, consulte a *Seção 10.2, "`initramfs`"*. Caso o sistema não tenha um disco rígido local, o `initramfs` deverá indicar o sistema de arquivos raiz ao Kernel. Isso pode ser feito com a ajuda de um dispositivo de bloco de rede, como iSCSI ou SAN, mas também é possível usar o NFS como o dispositivo raiz.

Nota: A nomeação de processo do `init`

Dois programas diferentes são comumente chamados "init":

a. o processo `initramfs`, que monta o sistema de arquivos raiz

b. o processo do sistema operacional, que configura o sistema

Neste capítulo, vamos chamá-los de "`init` no `initramfs`" e de "`systemd`", respectivamente.

4. **init no initramfs.** Este programa executa todas as ações necessárias para montar o sistema de arquivos raiz apropriado. Ele dispõe da funcionalidade do Kernel para o sistema de arquivos necessário e de drivers do dispositivo para controladoras de armazenamento em massa com o `udev`. Uma vez encontrado o sistema de arquivos raiz, ele é verificado quanto a erros e montado. Se esse procedimento for bem-sucedido, o `initramfs` será limpo e o daemon `systemd` no sistema de arquivos raiz será executado. Para obter mais informações sobre o `init` no `initramfs`, consulte a *Seção 10.3, "init no `initramfs`"*. Há mais informações a respeito do `udev` no *Capítulo 17, Gerenciamento dinâmico de dispositivos do Kernel com `udev`*.

5. **`systemd`.** Ao iniciar serviços e montar sistemas de arquivos, o `systemd` controla a inicialização real do sistema. O `systemd` está descrito no *Capítulo 11, O daemon `systemd`*.

10.2 initramfs

O `initramfs` é um pequeno arquivo cpio que pode ser carregado pelo Kernel em um disco RAM. Ele fornece um ambiente Linux mínimo que permite a execução de programas antes da montagem do sistema de arquivos raiz. Este ambiente mínimo do Linux é carregado na memória pelas rotinas do BIOS ou da UEFI e não tem outros requisitos de hardware específicos além de memória suficiente. O arquivo `initramfs` sempre deve incluir um executável denominado `init`, que executa o daemon `systemd` no sistema de arquivos raiz para realização do processo de boot.

Antes da montagem do sistema de arquivos raiz e da inicialização do sistema operacional, o Kernel precisa dos drivers correspondentes para acessar o dispositivo em que o sistema de arquivos raiz está localizado. Esses drivers podem incluir drivers especiais para determinados tipos de unidades de discos rígidos ou até drivers de rede para acesso a um sistema de arquivos de rede. Os módulos necessários para o sistema de arquivos raiz podem ser carregados pelo `init` no `initramfs`. Depois de carregados os módulos, o `udev` fornecerá os dispositivos necessários ao `initramfs`. Posteriormente no processo de boot, depois de mudar o sistema de arquivos raiz, será necessário gerar novamente os dispositivos. Isso é feito pela unidade do `systemd` `udev.service`, com o comando **`udevtrigger`**.

Se você precisar mudar o hardware (por exemplo, discos rígidos) em um sistema instalado e esse hardware exigir a presença de drivers diferentes no Kernel durante a inicialização, será necessário atualizar o arquivo `initramfs`. Para fazer isso, chame **`dracut -f`** (a opção `-f` sobregrava o arquivo initramfs existente). Para adicionar um driver para o novo hardware, edite `/etc/dracut.conf.d/01-dist.conf` e adicione a linha a seguir.

```
force_drivers+="driver1"
```

Substitua *`driver1`* pelo nome do driver do módulo. Se for necessário adicionar mais do que um driver, liste-os separados com espaço (*`driver1 driver2`*.

Importante: Atualizando o `initramfs` ou o `init`

O carregador de boot carrega o `initramfs` ou o `init` da mesma maneira que o Kernel. Não será necessário reinstalar o GRUB 2 após atualizar o `initramfs` ou o `init`, pois o GRUB 2 procura o arquivo certo no diretório durante a inicialização.

10.3 init no `initramfs`

O principal objetivo do `init` no `initramfs` é preparar a montagem e o acesso ao sistema de arquivos raiz real. Dependendo da configuração do sistema, o `init` no `initramfs` será responsável pelas tarefas a seguir.

Carregamento de módulos Kernel

Dependendo da configuração do hardware, drivers especiais poderão ser necessários para acessar os componentes de hardware do computador (sendo que o componente mais importante é o disco rígido). Para acessar o sistema de arquivos raiz final, o Kernel precisa carregar os drivers adequados do sistema de arquivos.

Fornecendo arquivos especiais de bloco

Para cada módulo carregado, o Kernel gera eventos de dispositivo. O `udev` gerencia esses eventos e gera os arquivos de bloco especiais necessários em um sistema de arquivos RAM em `/dev`. Sem esses arquivos especiais, o sistema de arquivos e outros dispositivos não estariam acessíveis.

Gerenciamento de configurações RAID e LVM

Se você configurar o sistema para armazenar o sistema de arquivos raiz no RAID ou no LVM, o `init` no `initramfs` configurará o LVM ou o RAID para permitir acesso ao sistema de arquivos raiz posteriormente. Obtenha informações sobre RAID e LVM no *Book "*Deployment Guide*" 12 "Advanced Disk Setup"*.

Gerenciamento de conexões de rede

Se você configurar o sistema para usar um sistema de arquivos raiz montado em rede (via NFS), o `init` no `initramfs` deverá verificar se os drivers de rede apropriados foram carregados e configurados para permitir acesso ao sistema de arquivos raiz.

Se o sistema de arquivos residir em um dispositivo de blocos em rede, como iSCSI ou SAN, a conexão com o servidor de armazenamento também será configurada pelo `init` no `initramfs`.

Quando o `init` no `initramfs` é chamado durante o boot inicial como parte do processo de instalação, suas tarefas são diferentes das que foram mencionadas acima:

Localização da mídia de instalação

Ao iniciar o processo de instalação, a máquina carrega um Kernel de instalação e um `init` especial que inclui o instalador do YaST. O instalador do YaST é executado em um sistema de arquivos RAM e precisa ter informações sobre a localização do meio de instalação para acessá-lo e instalar o sistema operacional.

Inicialização do reconhecimento de hardware e carregamento dos módulos kernel adequados

Como mencionado na *Seção 10.2, "`initramfs`"*, o processo de boot é iniciado com um conjunto mínimo de drivers que pode ser usado com a maioria das configurações de hardware. O `init` inicia um processo de exploração de hardware que determina o conjunto de drivers adequado à sua configuração de hardware. Esses drivers são usados para gerar um `initramfs` personalizado necessário para inicializar o sistema. Se os módulos não forem necessários para inicialização, mas forem para coldplug, eles poderão ser carregados com `systemd`. Para obter mais informações, consulte a *Seção 11.6.3, "Carregamento de módulos Kernel"*.

Carregando o sistema de instalação

Os drivers apropriados serão carregados logo após o reconhecimento adequado do hardware. O programa `udev` cria os arquivos de dispositivo especiais, e o `init` inicia o sistema de instalação com o instalador do YaST.

Inicialização do YaST

Por fim, o `init` inicia o YaST, que inicia a instalação do pacote e a configuração do sistema.

11 O daemon `systemd`

O programa `systemd` tem ID de processo 1. Ele é responsável por inicializar o sistema da forma exigida. O `systemd` é iniciado diretamente pelo Kernel e resiste ao sinal 9, que normalmente termina os processos. Todos os outros programas são iniciados diretamente pelo systemd ou por um de seus processos filho.

Desde o SUSE Linux Enterprise Desktop 12, o systemd é o substituto do popular daemon init do System V. O `systemd` é totalmente compatível com o init do System V (pois suporta scripts init). Uma das vantagens principais do systemd é que ele acelera consideravelmente o tempo de boot, devido à sua capacidade agressiva de paralelização para iniciar serviços. Além disso, o systemd apenas inicia um serviço quando é realmente necessário. Os daemons não são iniciados incondicionalmente no momento da inicialização, mas, em vez disso, quando são solicitados pela primeira vez. O systemd também suporta Grupos de Controle do Kernel (cgroups), criação de instantâneos, restauração do estado do sistema, etc. Consulte http://www.freedesktop.org/wiki/Software/systemd/ para obter os detalhes.

11.1 O conceito do systemd

Esta seção apresenta detalhes sobre o conceito que rege o systemd.

11.1.1 O que é systemd

O systemd é um gerenciador de sistema e sessão para Linux, compatível com os scripts init do System V e do LSB. Os principais recursos são:

- capacidade agressiva de paralelização
- uso de soquete e ativação por D-Bus para iniciar serviços
- capacidade de iniciar daemons sob demanda
- acompanhamento de processos usando cgroups do Linux
- suporte à criação de instantâneos e restauração do estado do sistema
- manutenção dos pontos de montagem e automount
- implementação de uma lógica elaborada de controle de serviço baseada em dependência transacional

11.1.2 Arquivo unit

O arquivo de configuração unit codifica as informações sobre serviço, soquete, dispositivo, ponto de montagem, ponto de automount, arquivo de troca ou partição, destino de inicialização, caminho do sistema de arquivos monitorado, temporizador controlado e supervisionado pelo systemd, instantâneo de estado do sistema temporário, fração de gerenciamento de recursos ou grupo de processos criados externamente. O “arquivo unit” é um termo genérico usado pelo systemd para o seguinte:

- **Serviço.** Informações sobre um processo (por exemplo, a execução de um daemon); o arquivo termina com .service
- **Destinos.** Usado para agrupar unidades e como pontos de sincronização durante a inicialização; o arquivo termina com .target
- **Soquetes.** Informações sobre um soquete de rede, IPC ou FIFO do sistema de arquivos, para ativação baseada em soquete (como `inetd`); o arquivo termina com .socket
- **Caminho.** Usado para acionar outras unidades (por exemplo, executar um serviço quando houver mudanças nos arquivos); o arquivo termina com .path
- **Timer.** Informações sobre um temporizador controlado, para ativação baseada em temporizador; o arquivo termina com .timer
- **Ponto de montagem.** Normalmente, gerado de forma automática pelo gerador fstab; o arquivo termina com .mount
- **Ponto de automount.** Informações sobre um ponto de automount do sistema de arquivos; o arquivo termina com .automount
- **Swap.** Informações sobre um dispositivo ou arquivo de troca para paginação de memória; o arquivo termina com .swap
- **Dispositivo.** Informações sobre uma unidade de dispositivo conforme exposta na árvore de dispositivos do sysfs/udev(7); o arquivo termina com .device
- **Escopo/Fração.** Um conceito de gerenciamento hierárquico de recursos de um grupo de processos; o arquivo termina com .scope/.slice

Para obter mais informações sobre o systemd.unit, consulte http://www.freedesktop.org/software/systemd/man/systemd.unit.html

11.2 Uso básico

O sistema init do System V usa vários comandos diferentes para gerenciar os serviços: scripts init, **`insserv`**, **`telinit`** e outros. O systemd facilita gerenciar serviços, já que existe apenas um comando para memorizar para a maioria das tarefas de gerenciamento de serviços: **`systemctl`**. Ele usa a notação "command plus subcommand", como **`git`** ou **`zypper`**:

```
systemctl [general OPTIONS] subcommand [subcommand OPTIONS]
```

Consulte **`man 1 systemctl`** para obter o manual completo.

Dica: Saída de terminal e complementação bash

Se a saída chegar a um terminal (e não a um pipe ou arquivo, por exemplo), por padrão, os comandos systemd enviarão uma saída extensa para um pager. Use a opção `--no-pager` para desativar o modo de paginação.

O systemd também suporta a complementação bash, que permite digitar as primeiras letras de um subcomando e pressionar ⇥ para completá-lo automaticamente. Esse recurso está disponível apenas no shell `bash` e requer a instalação do pacote `bash-completion`.

11.2.1 Gerenciando serviços em um sistema em execução

Os subcomandos de gerenciamento de serviços são os mesmos usados para gerenciar um serviço com o init do System V (**`start`**, **`stop`**, etc.). A sintaxe geral dos comandos de gerenciamento de serviços é a seguinte:

systemd

```
systemctl reload|restart|start|status|stop|... <my_service(s)>.service
```

Init do System V

```
rc<my_service(s)> reload|restart|start|status|stop|...
```

O systemd permite gerenciar vários serviços de uma só vez. Em vez de executar os scripts init um após o outro como acontece com o init do System V, execute um comando da seguinte forma:

```
systemctl start <my_1st_service>.service <my_2nd_service>.service
```

Para listar todos os serviços disponíveis no sistema:

```
systemctl list-unit-files --type=service
```

A tabela a seguir lista os comandos de gerenciamento de serviços mais importantes para o systemd e o init do System V:

TABELA 11.1 COMANDOS DE GERENCIAMENTO DE SERVIÇOS

Tarefa	Comando systemd	Comando init do System V
Iniciando.	`start`	`start`
Parar.	`stop`	`stop`
Reiniciar. Encerra os serviços e os inicia na sequência. Se algum serviço ainda não estiver em execução, ele será iniciado.	`restart`	`restart`
Reiniciar condicionalmente. Reinicia os serviços se já estiverem em execução. Não faz nada para os serviços que não estão em execução.	`try-restart`	`try-restart`
Recarregar. Instrui os serviços a recarregarem seus arquivos de configuração sem interromper a operação. Caso de uso: Instruir o Apache a recarregar um arquivo de configuração `httpd.conf` modificado. Observe que nem todos os serviços suportam recarregamento.	`reload`	`reload`
Recarregar ou reiniciar. Recarrega os serviços quando o recarregamento é	`reload-or-restart`	`n/a`

Tarefa	Comando systemd	Comando init do System V
suportado; do contrário, reinicia-os. Se algum serviço ainda não estiver em execução, ele será iniciado.		
Recarregar ou reiniciar condicionalmente. Recarrega os serviços se o recarregamento for suportado; do contrário reinicia-os, se estiverem em execução. Não faz nada para os serviços que não estão em execução.	`reload-or-try-restart`	`n/a`
Obter informações detalhadas sobre status. Lista as informações sobre o status dos serviços. O comando `systemd` mostra detalhes, como descrição, executável, status, cgroup e as últimas mensagens emitidas por um serviço (consulte a *Seção 11.6.6, "Depurando serviços"*). O nível dos detalhes exibidos com o init do System V varia de acordo com cada serviço.	`status`	`status`
Obter informações resumidas sobre status. Mostra se os serviços estão ou não ativos.	`is-active`	`status`

11.2.2 Habilitando/Desabilitando serviços permanentemente

Os comandos de gerenciamento de serviços mencionados na seção anterior permitem manipular serviços na seção atual. O systemd também permite habilitar ou desabilitar serviços permanentemente para serem iniciados automaticamente quando solicitados ou para ficarem sempre indisponíveis. É possível fazer isso com o YaST ou por linha de comando.

11.2.2.1 Habilitar/Desabilitar serviços na linha de comando

A tabela a seguir lista os comandos de habilitação e desabilitação pelo systemd e pelo init do System V:

Importante: Inicialização de serviço

Ao habilitar um serviço na linha de comando, ele não é iniciado automaticamente. Ele é programado para iniciar na próxima inicialização do sistema ou mudança de nível de execução/destino. Para iniciar um serviço logo após ele ter sido habilitado, execute **`systemctl start <meu_serviço>.service`** ou **`rc<meu_serviço> start`** explicitamente.

TABELA 11.2 COMANDOS PARA HABILITAR E DESABILITAR SERVIÇOS

Tarefa	Comando systemd	Comando init do System V
Habilitando.	**`systemctl enable`** *`<meu(s)_serviço(s)>`***`.service`**	**`insserv`** *`<meu(s)_serviço(s)>`*
Desabilitar.	**`systemctl disable`** *`<meu(s)_serviço(s)>`***`.service`**	**`insserv -r`** *`<meu(s)_serviço(s)>`*
Verificar. Mostra se um serviço está ou não habilitado.	**`systemctl is-enabled`** *`<meu_serviço>`***`.service`**	n/d
Reabilitar. Semelhante a reiniciar um serviço, este comando primeiro desabilita e depois habilita um serviço. Útil para restaurar um serviço aos seus padrões.	**`systemctl reenable`** *`<meu_serviço>`***`.service`**	n/d
Mascarar. Após “desabilitar” um serviço, ele ainda poderá ser iniciado manualmente.	**`systemctl mask`** *`<meu_serviço>`***`.service`**	n/d

Tarefa	`Comando systemd`	Comando init do System V
Para desabilitar um serviço completamente, é necessário mascará-lo. Use com cuidado.		
Desmascarar. Só será possível usar novamente um serviço mascarado depois que ele for desmascarado.	**`systemctl unmask`** *`<meu_serviço>`***`.service`**	n/d

11.3 Inicialização do sistema e gerenciamento de destino

Todo o processo de inicialização e encerramento do sistema é mantido pelo systemd. Desse ponto de vista, o Kernel pode ser considerado um processo em segundo plano para manter todos os outros processos e ajustar o tempo de CPU e o acesso ao hardware de acordo com as solicitações de outros programas.

11.3.1 Destinos X níveis de execução

Com o init do System V, o sistema era inicializado no chamado “Nível de execução”. O nível de execução define como o sistema é iniciado e quais serviços estão disponíveis no sistema em execução. Os níveis de execução são numerados: os mais conhecidos são `0` (encerramento do sistema), `3` (multiusuário com rede) e `5` (multiusuário com rede e gerenciador de exibição).

O systemd apresenta um novo conceito usando as chamadas “unidades de destino”. No entanto, ele continua totalmente compatível com o conceito de nível de execução. As unidades de destino são nomeadas, e não numeradas, e possuem finalidades específicas. Por exemplo, os destinos `local-fs.target` e `swap.target` montam sistemas de arquivos locais e espaços de troca.

O destino `graphical.target` oferece recursos de sistema multiusuário com rede e gerenciador de exibição e equivale ao nível de execução 5. Destinos complexos, como `graphical.target`, agem como destinos "meta", combinando um subconjunto de outros destinos. Como o systemd facilita criar destinos personalizados combinando destinos existentes, ele oferece excelente flexibilidade.

A lista a seguir mostra as unidades de destino mais importantes do systemd. Para ver a lista completa, consulte **`man 7 systemd.special`**.

UNIDADES DE DESTINO SELECIONADAS DO SYSTEMD

`default.target`
: O destino que é inicializado por padrão. Não um destino "real", mas um link simbólico para outro destino, como `graphic.target`. Pode ser modificado permanentemente pelo YaST (consulte a *Seção 11.4, "Gerenciando serviços com o YaST"*). Para mudá-lo em uma sessão, use a opção de linha de comando do Kernel `systemd.unit=<meu_destino>.destino` no prompt de boot.

`emergency.target`
: Inicia o shell de emergência no console. Use-o apenas no prompt de boot como `systemd.unit=emergency.target`.

`graphical.target`
: Inicia um sistema com suporte a rede multiusuário e um gerenciador de exibição.

`halt.target`
: Encerra o sistema.

`mail-transfer-agent.target`
: Inicia todos os serviços necessários para enviar e receber e-mails.

`multi-user.target`
: Inicia um sistema multiusuário com rede.

`reboot.target`
: Reinicializa o sistema.

`rescue.target`
: Inicia um sistema de usuário único sem rede.

Para continuar compatível com o sistema de nível de execução init do System V, o systemd oferece destinos especiais chamados `runlevelX.target` mapeados a níveis de execução correspondentes numerados `X`.

Para saber o destino atual, use o comando: **`systemctl get-default`**

TABELA 11.3 NÍVEIS DE EXECUÇÃO DO SYSTEM V E UNIDADES DE DESTINO DO `systemd`

Nível de execução do System V	Destino do `systemd`	Finalidade
0	`runlevel0.target`, `halt.target`, `poweroff.target`	Encerramento do sistema
1, S	`runlevel1.target`, `rescue.target`,	Modo de usuário único
2	`runlevel2.target`, `multi-user.target`,	Multiusuário local sem rede remota
3	`runlevel3.target`, `multi-user.target`,	Multiusuário completo com rede
4	`runlevel4.target`	Não usado/Definido pelo usuário
5	`runlevel5.target`, `graphical.target`,	Multiusuário completo com rede e gerenciador de exibição
6	`runlevel6.target`, `reboot.target`,	Reinicialização do sistema

Importante: O systemd ignora o `/etc/inittab`

Os níveis de execução em um sistema init do System V são configurados em `/etc/inittab`. O systemd *não* usa essa configuração. Consulte a *Seção 11.5.3, "Criando destinos personalizados"* para obter instruções sobre como criar seu próprio destino inicializável.

11.3.1.1 Comandos para mudar os destinos

Use os seguintes comandos para operar com unidades de destino:

Tarefa	Comando systemd	Comando init do System V
Mudar o destino/nível de execução atual	**`systemctl isolate`** *<meu_destino>*`.target`	**`telinit`** *X*
Mudar para o destino/nível de execução padrão	**`systemctl default`**	n/d
Obter o destino/nível de execução atual	**`systemctl list-units --type=target`** Com o systemd, normalmente há mais de um destino ativo. O comando lista todos os destinos que estão ativos.	**`who -r`** ou **`runlevel`**
Mudar o nível de execução padrão de forma persistente	Use o Gerenciador de Serviços ou execute o seguinte comando: **`ln -sf /usr/lib/systemd/system/`***<meu_destino>*`.target /etc/systemd/system/default.target`**	Use o Gerenciador de Serviços ou mude a linha **`id:`***X*`:initdefault:`** em `/etc/inittab`
Mudar o nível de execução padrão para o processo de boot atual	Digite a seguinte opção no prompt de boot **`systemd.unit=`***<meu_destino>*`.target`**	Digite o número do nível de execução desejado no prompt de boot.
Mostrar as dependências de um destino/nível de execução	**`systemctl show -p "Requires"`** *<meu_destino>*`.target` **`systemctl show -p "Wants"`** *<meu_destino>*`.target`	n/d

Tarefa	Comando systemd	Comando init do System V
	“Requires” lista as dependências obrigatórias (hard) (aquelas que devem ser resolvidas), enquanto “Wants” lista as dependências desejadas (soft) (aquelas que são resolvidas quando possível).	

11.3.2 Depurando a inicialização do sistema

O systemd oferece os meios para a análise dos processos de inicialização do sistema. É possível revisar a lista de todos os serviços e status de forma prática (sem ter que analisar o `/varlog/`). O systemd permite também explorar o procedimento de inicialização para descobrir quanto tempo leva para inicializar cada serviço.

11.3.2.1 Revisar inicialização dos serviços

Para revisar a lista completa dos serviços que foram iniciados desde a inicialização do sistema, digite o comando **`systemctl`**. Ele lista todos os serviços ativos, conforme mostrado a seguir (resumidamente). Para obter mais informações sobre determinado serviço, use **`systemctl status`** *<meu_serviço>*`.service`.

EXEMPLO 11.1 LISTAR SERVIÇOS ATIVOS

```
root # systemctl
UNIT                                LOAD   ACTIVE SUB       JOB DESCRIPTION
[...]
systemd-random-seed-load.path       loaded active waiting       Random Seed
acpid.service                       loaded active running       ACPI Event Daemon
apache2.service                     loaded failed failed        apache
avahi-daemon.service                loaded active running       Avahi mDNS/DNS-SD
 Stack
bluez-coldplug.service              loaded active exited        LSB: handles udev
 coldplug of bluetooth dongles
```

```
console-kit...-system-start.service loaded active exited        Console System
 Startup Logging
cron.service                       loaded active running       Command Scheduler
cups.service                       loaded active running       CUPS Printing
 Service
[...]
LOAD   = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB    = The low-level unit activation state, values depend on unit type.
JOB    = Pending job for the unit.

107 units listed. Pass --all to see inactive units, too.
```

Para restringir o resultado a serviços com falha na inicialização, use a opção `--failed`:

EXEMPLO 11.2 LISTAR SERVIÇOS COM FALHA

```
root # systemctl --failed
UNIT                    LOAD   ACTIVE SUB    JOB DESCRIPTION
apache2.service         loaded failed failed     apache
NetworkManager.service loaded failed failed     Network Manager
plymouth-start.service loaded failed failed     Show Plymouth Boot Screen

[...]
```

11.3.2.2 Depurar o tempo de inicialização

Para depurar o tempo de inicialização do sistema, o systemd oferece o comando **`systemd-analyze`**. Ele mostra o tempo total de inicialização, uma lista dos serviços solicitados por tempo de inicialização e também gera um gráfico SVG mostrando o tempo que os serviços levaram para serem iniciados em relação a outros serviços.

Listando o tempo de inicialização do sistema

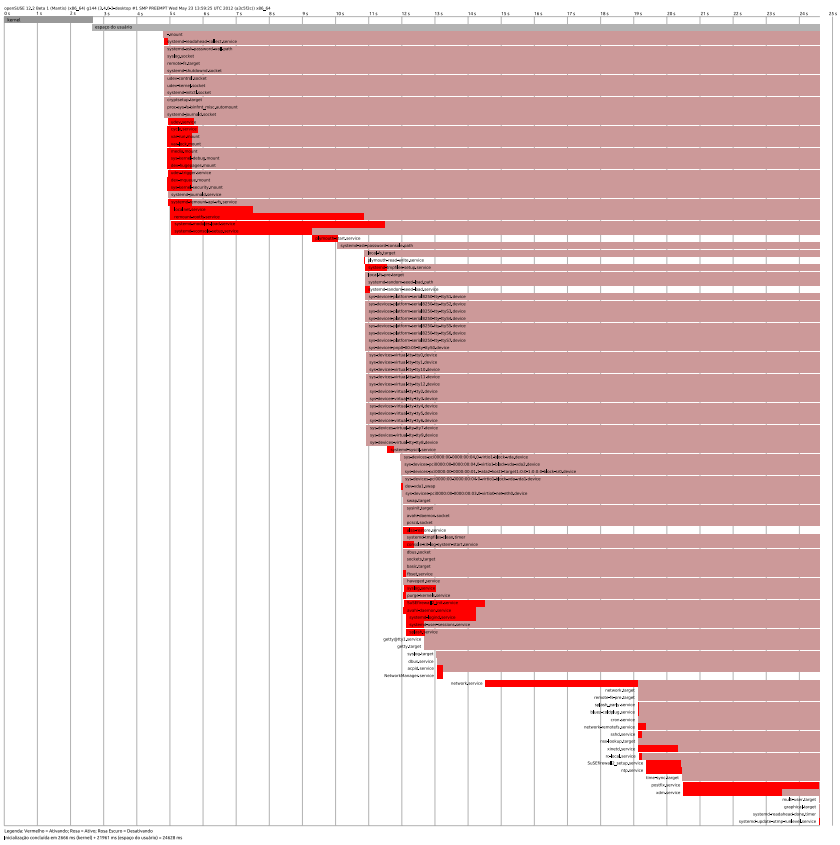
```
root # systemd-analyze
Startup finished in 2666ms (kernel) + 21961ms (userspace) = 24628ms
```

Listando o tempo de inicialização dos serviços

```
root # systemd-analyze blame
  6472ms systemd-modules-load.service
  5833ms remount-rootfs.service
  4597ms network.service
  4254ms systemd-vconsole-setup.service
  4096ms postfix.service
  2998ms xdm.service
  2483ms localnet.service
  2470ms SuSEfirewall2_init.service
  2189ms avahi-daemon.service
  2120ms systemd-logind.service
  1210ms xinetd.service
  1080ms ntp.service
[...]
    75ms fbset.service
    72ms purge-kernels.service
    47ms dev-vda1.swap
    38ms bluez-coldplug.service
    35ms splash_early.service
```

Gráficos do tempo de inicialização dos serviços

```
root # systemd-analyze plot > jupiter.example.com-startup.svg
```



11.3.2.3 Revisar o processo de inicialização completo

Os comandos mencionados anteriormente permitem revisar os serviços que foram iniciados e o tempo que levou para iniciá-los. Se você precisar de mais detalhes, poderá instruir o `systemd` a registrar de forma verbosa o procedimento de inicialização completo, digitando os seguintes parâmetros no prompt de boot:

```
systemd.log_level=debug systemd.log_target=kmsg
```

Agora o `systemd` grava suas mensagens de registro no buffer de anel do kernel. Veja esse buffer com **`dmesg`**:

```
dmesg -T | less
```

11.3.3 Compatibilidade com o System V

O Systemd é compatível com o System V, o que ainda permite usar os scripts init existentes do System V. Entretanto, há pelo menos um problema conhecido em que o script init do System V não funciona com o Systemd out-of-the-box: iniciar um serviço como outro usuário por meio de **`su`** ou **`sudo`** nos scripts init resulta em falha do script, gerando um erro de "Acesso negado". Ao mudar o usuário com **`su`** ou **`sudo`**, é iniciada uma sessão PAM. Essa sessão será terminada após a conclusão do script init. Como consequência, o serviço que foi iniciado pelo script init também será terminado. Para solucionar esse erro, faça o seguinte:

1. Crie um agrupador de arquivo de serviço com o mesmo nome do script init e mais a extensão de nome de arquivo `.service`:

   ```
   [Unit]
   Description=DESCRIPTION
   After=network.target

   [Service]
   User=USER
   Type=forking (1)
   PIDFile=PATH TO PID FILE (1)
   ExecStart=PATH TO INIT SCRIPT start
   ExecStop=PATH TO INIT SCRIPT stop
   ExecStopPost=/usr/bin/rm -f PATH TO PID FILE (1)

   [Install]
   WantedBy=multi-user.target (2)
   ```

   Substitua todos os valores gravados em *`LETRAS MAIÚSCULAS`* pelos valores apropriados.

   (1) Opcional: use apenas se o script init iniciar um daemon.

   (2) O `multi-user.target` também inicia o script init ao inicializar no `graphical.target`. Se ele tiver que ser iniciado apenas ao inicializar no gerenciador de exibição, use o `graphical.target` aqui.

2. Inicie o daemon com **`systemctl start`** *`APLICATIVO`***`.service`**

11.4 Gerenciando serviços com o YaST

O gerenciamento básico de serviços também pode ser feito com o módulo Gerenciador de Serviços do YaST. Ele permite iniciar, parar, habilitar e desabilitar serviços. Ele permite também mostrar o status e mudar o destino padrão de um serviço. Inicie o módulo do YaST em *YaST* › *Sistema* › *Services Manager* (Gerenciador de Serviços).

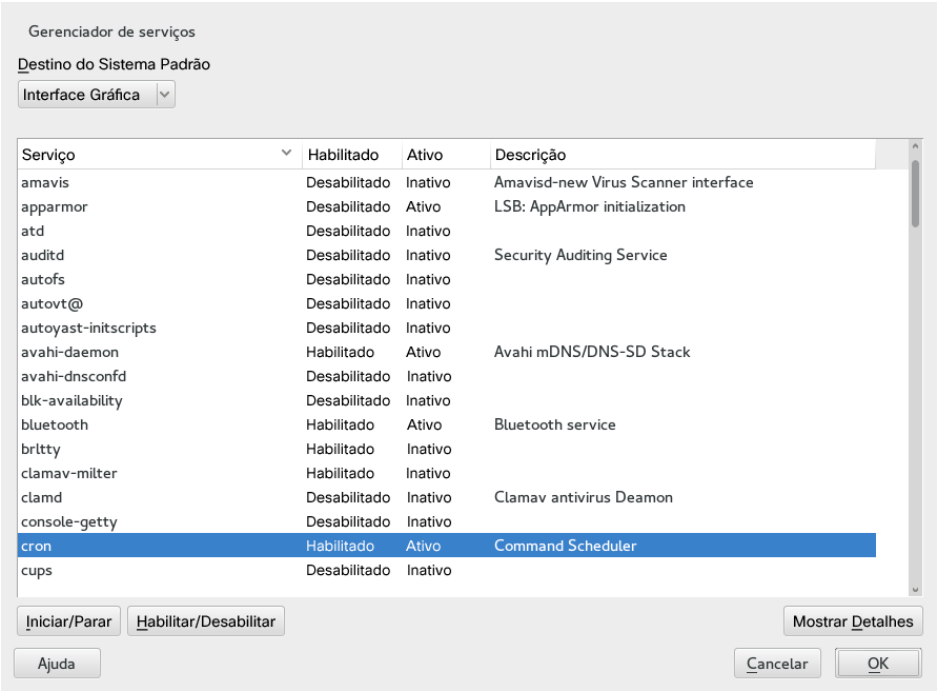


FIGURA 11.1 GERENCIADOR DE SERVIÇOS

Mudando o *destino padrão do sistema*

Para mudar o destino de inicialização do sistema, escolha o destino na caixa suspensa *Default System Target* (Destino Padrão do Sistema). Os destinos mais usados são *Graphical Interface* (Interface Gráfica) (iniciando uma tela gráfica de login) e *Multiusuário* (iniciando o sistema no modo de linha de comando).

Iniciando ou parando um serviço

Selecione um serviço da tabela. A coluna *Ativo* mostra se ele está em execução (*Ativo*) ou não (*Inativo*). Para alternar o status, escolha *Iniciar/Parar*.

Quando um serviço é iniciado ou parado, seu status muda na sessão que está em execução. Para mudar seu status em todas as reinicializações, é necessário habilitá-lo ou desabilitá-lo.

Habilitando ou desabilitando um serviço

Selecione um serviço da tabela. A coluna *Habilitado* mostra se ele está *Habilitado* ou *Desabilitado*. Para alternar o status, escolha *Habilitar/Desabilitar*.

Quando um serviço é habilitado ou desabilitado, você configura se ele deve ser iniciado durante a inicialização (*Habilitado*) ou não (*Desabilitado*). Essa configuração não afeta a sessão atual. Para mudar seu status na sessão atual, é necessário iniciá-lo ou pará-lo.

Ver mensagens de status

Para ver a mensagem de status de um serviço, selecione-o na lista e escolha *Mostrar Detalhes*. A saída exibida será idêntica a que foi gerada pelo comando `systemctl -l status <meu_serviço>`.

Atenção: Configurações de nível de execução defeituosas podem danificar o sistema

Configurações de nível de execução defeituosas podem tornar o sistema inutilizável. Antes de aplicar as mudanças, tenha absoluta certeza sobre suas consequências.

11.5 Personalização do `systemd`

As seções a seguir mostram alguns exemplos de personalizações do `systemd`.

Atenção: Evitando sobregravar personalizações

Faça sempre as personalizações do systemd em `/etc/systemd/`, *nunca* em `/usr/lib/systemd/`. Do contrário, as mudanças serão sobregravadas na próxima atualização do systemd.

11.5.1 Personalizando arquivos de serviço

Os arquivos de serviço do systemd estão localizados em `/usr/lib/systemd/system`. Para personalizá-los, faça o seguinte:

1. Copie os arquivos que deseja modificar de `/usr/lib/systemd/system` para `/etc/systemd/system`. Mantenha os mesmos nomes de arquivo dos originais.

2. Modifique as cópias em `/etc/systemd/system` de acordo com as suas necessidades.

3. Para obter uma visão geral das mudanças de configuração, use o comando **`systemd-delta`**. Ele compara e identifica os arquivos de configuração que anulam outros arquivos de configuração. Para obter detalhes, consulte a página de manual do **`systemd-delta`**.

Os arquivos modificados em `/etc/systemd` terão prioridade sobre os arquivos originais em `/usr/lib/systemd/system`, desde que seus nomes sejam iguais.

11.5.2 Criando arquivos “dropin”

Para adicionar apenas algumas linhas a um arquivo de configuração ou modificar uma pequena parte dele, é possível usar os chamados arquivos “dropin”. Esses arquivos permitem estender a configuração dos arquivos de unidade sem ter que editá-los ou anulá-los realmente.

Por exemplo, para mudar um valor no serviço *`foobar`* localizado em `/usr/lib/systemd/system/ foobar.service`, faça o seguinte:

1. Crie um diretório chamado `/etc/systemd/system/<meu_serviço>.service.d/`. Observe o sufixo `.d`. O diretório deve receber outro nome de acordo com o serviço que você deseja corrigir com o arquivo dropin.

2. Nesse diretório, crie um arquivo *`qualquermodificação`*`.conf`. Verifique se ele contém somente a linha com o valor que deseja modificar.

3. Grave as mudanças feitas no arquivo Ele será usado como extensão do arquivo original.

11.5.3 Criando destinos personalizados

Nos sistemas init SUSE do System V, o nível de execução 4 não costuma ser usado para permitir que administradores criem sua própria configuração de nível de execução. O systemd permite criar qualquer número de destinos personalizados. A sugestão é começar adaptando um destino existente, como `graphical.target`.

1. Copie o arquivo de configuração `/usr/lib/systemd/system/graphical.target` para `/etc/systemd/system/<meu_destino>.target` e ajuste-o de acordo com as suas necessidades.

2. O arquivo de configuração copiado na etapa anterior já inclui as dependências obrigatórias (“hard”) do destino. Para incluir também as dependências desejadas (“soft”), crie um diretório `/etc/systemd/system/<meu_destino>.target.wants`.

3. Para cada serviço desejado, crie um link simbólico de `/usr/lib/systemd/system` para `/etc/systemd/system/<meu_destino>.target.wants`.

4. Após concluir a configuração do destino, recarregue a configuração do systemd para disponibilizar o novo destino:

```
systemctl daemon-reload
```

11.6 Uso avançado

As seções a seguir abordam tópicos avançados para administradores do sistema. Para obter uma documentação ainda mais avançada do systemd, consulte a série de Lennart Pöttering sobre o systemd para administradores em http://0pointer.de/blog/projects.

11.6.1 Registro do Sistema

A *Seção 11.6.6, “Depurando serviços”* explica como ver mensagens de registro de determinado serviço. No entanto, a exibição de mensagens de registro não se restringe a registros de serviços. É possível também acessar e consultar as mensagens de registro completas gravadas pelo `systemd`, o chamado “Diário”. Use o comando **`systemd-journalctl`** para exibir as mensagens de registro completas com as entradas antigas. Consulte **`man 1 systemd-journalctl`** para ver as opções; por exemplo, aplicação de filtros ou mudança do formato de saída.

11.6.2 Instantâneos

É possível gravar o estado atual do `systemd` em um instantâneo nomeado e mais tarde revertê-lo com o subcomando **`isolate`**. Isso é útil para testar serviços ou destinos personalizados, pois permite retornar para um estado definido a qualquer momento. Um instantâneo só fica disponível na sessão atual e é apagado automaticamente na reinicialização. O nome do instantâneo deve terminar com `.snapshot`.

Criar um instantâneo

```
systemctl snapshot <my_snapshot>.snapshot
```

Apagar um instantâneo

```
systemctl delete <my_snapshot>.snapshot
```

Ver um instantâneo

```
systemctl show <my_snapshot>.snapshot
```

Ativar um instantâneo

```
systemctl isolate <my_snapshot>.snapshot
```

11.6.3 Carregamento de módulos Kernel

Com o `systemd`, é possível carregar os módulos do kernel automaticamente no momento da inicialização, usando o arquivo de configuração em

- `/usr/lib/modules-load.d` e
- `/etc/modules-load.d`

Para obter mais informações, consulte a página de manual `modules-load.d(5)`.

11.6.4 Grupos de controle (cgroups) do Kernel

Em um sistema init tradicional do System V, nem sempre é possível atribuir claramente um processo ao serviço que o gerou. Alguns serviços, como o Apache, geram diversos processos de terceiros (por exemplo, processos CGI ou Java) que, por sua vez, geram mais processos. Isso dificulta ou até impossibilita uma atribuição clara. Além do mais, um serviço pode não terminar corretamente, deixando alguns filhos ativos.

O systemd resolve este problema colocando cada serviço em seu próprio grupo de controle (cgroup). Cgroups são recursos do Kernel que possibilitam agregar processos e todos os seus filhos em grupos hierárquicos organizados. O systemd nomeia cada cgroup de acordo com seu serviço. Como um processo não privilegiado não pode "deixar" seu cgroup, essa é uma forma eficiente de rotular todos os processos gerados por um serviço com o nome do serviço.

Para listar todos os processos pertencentes a um serviço, use o comando **`systemd-cgls`**. O resultado será parecido com o seguinte exemplo (resumido):

EXEMPLO 11.3 LISTAR TODOS OS PROCESSOS PERTENCENTES A UM SERVIÇO

```
root # systemd-cgls --no-pager
├─1 /usr/lib/systemd/systemd --switched-root --system --deserialize 20
├─user.slice
│ └─user-1000.slice
│   ├─session-102.scope
│   │ ├─12426 gdm-session-worker [pam/gdm-password]
│   │ ├─15831 gdm-session-worker [pam/gdm-password]
│   │ ├─15839 gdm-session-worker [pam/gdm-password]
│   │ ├─15858 /usr/lib/gnome-terminal-server

[...]

└─system.slice
  ├─systemd-hostnamed.service
  │ └─17616 /usr/lib/systemd/systemd-hostnamed
  ├─cron.service
  │ └─1689 /usr/sbin/cron -n
  ├─ntpd.service
  │ └─1328 /usr/sbin/ntpd -p /var/run/ntp/ntpd.pid -g -u ntp:ntp -c /etc/ntp.conf
  ├─postfix.service
  │ ├─ 1676 /usr/lib/postfix/master -w
  │ ├─ 1679 qmgr -l -t fifo -u
  │ └─15590 pickup -l -t fifo -u
  ├─sshd.service
  │ └─1436 /usr/sbin/sshd -D
```

```
[...]
```

Consulte o *Book "*System Analysis and Tuning Guide*" 8 "Kernel Control Groups"* para obter mais informações sobre os cgroups.

11.6.5 Terminando os serviços (enviando sinais)

Conforme explicado na *Seção 11.6.4, "Grupos de controle (cgroups) do Kernel"*, nem sempre é possível atribuir um processo a seu processo de serviço pai em um sistema init do System V. Isso dificulta terminar um serviço e todos os seus filhos. Os processos filhos que não forem terminados permanecerão como processos zumbis.

O conceito do systemd de confinar cada serviço em um cgroup possibilita identificar claramente todos os processos filhos de um serviço e, portanto, permite enviar um sinal a cada um desses processos. Use **`systemctl kill`** para enviar sinais aos serviços. Para ver uma lista dos sinais disponíveis, consulte **`man 7 signals`**.

Enviando `SIGTERM` para um serviço

`SIGTERM` é o sinal padrão que é enviado.

```
systemctl kill <my_service>.service
```

Enviando um *`SINAL`* para um serviço

Use a opção `-s` para especificar o sinal que deve ser enviado.

```
systemctl kill -s SIGNAL <my_service>.service
```

Selecionando processos

Por padrão, o comando **`kill`** envia o sinal para `todos` os processos do cgroup especificado. É possível restringi-lo ao processo `control` ou `main`. Este último, por exemplo, é útil para forçar um serviço a recarregar sua configuração enviando `SIGHUP`:

```
systemctl kill -s SIGHUP --kill-who=main <my_service>.service
```

11.6.6 Depurando serviços

Por padrão, o systemd não é muito verboso. Se um serviço for iniciado com êxito, nenhuma saída será gerada. Em caso de falha, uma breve mensagem de erro será exibida. Porém, o **`systemctl status`** oferece os meios de depurar a inicialização e operação de um serviço.

O systemd já vem com um mecanismo de registro (“The Journal” — O Diário) que registra as mensagens do sistema. Isso permite exibir as mensagens de serviço juntamente com as mensagens de status. O comando **`status`** funciona de forma parecida com o comando **`tail`** e também exibe as mensagens de registro em formatos diferentes, o que faz dele uma poderosa ferramenta de depuração.

Mostrar falha na inicialização de serviço

Sempre que um serviço falhar ao ser iniciado, use **`systemctl status`** *<meu_serviço>*`.service` para ver a mensagem detalhada do erro:

```
root # systemctl start apache2.service
Job failed. See system journal and 'systemctl status' for details.
root # systemctl status apache2.service
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled)
   Active: failed (Result: exit-code) since Mon, 04 Jun 2012 16:52:26 +0200;
 29s ago
   Process: 3088 ExecStart=/usr/sbin/start_apache2 -D SYSTEMD -k start
 (code=exited, status=1/FAILURE)
   CGroup: name=systemd:/system/apache2.service

Jun 04 16:52:26 g144 start_apache2[3088]: httpd2-prefork: Syntax error on line
205 of /etc/apache2/httpd.conf: Syntax error on li...alHost>
```

Mostrar as últimas *n* mensagens de serviço

O comportamento padrão do subcomando **`status`** é exibir as dez últimas mensagens emitidas por um serviço. Para mudar o número de mensagens exibidas, use o parâmetro `--lines=`*n*:

```
systemctl status ntp.service
systemctl --lines=20 status ntp.service
```

Mostrar as mensagens de serviço no modo de anexação

Para exibir um “fluxo ao vivo” das mensagens de serviço, use a opção `--follow`, que funciona como o **`tail -f`**:

```
systemctl --follow status ntp.service
```

Formato de saída das mensagens

O parâmetro `--output=`*`modo`* permite mudar o formato de saída das mensagens de serviço. Os modos mais importantes disponíveis são:

`short`

O formato padrão. Mostra as mensagens de registro com uma marcação de horário legível.

`verbose`

Saída completa com todos os campos.

`cat`

Saída resumida sem marcações de horário.

11.7 Mais informações

Para obter mais informações sobre o systemd, consulte os seguintes recursos online:

Home page

http://www.freedesktop.org/wiki/Software/systemd

systemd para administradores

Lennart Pöttering, um dos criadores do systemd, escreveu uma série de entradas de blog (13 até o fechamento deste capítulo). Encontre-os em http://0pointer.de/blog/projects.

Centro de Controle: O sistema init do Linux `systemd`

http://www.h-online.com/open/features/Control-Centre-The-systemd-Linux-init-system-1565543.html

Inicialização: Ferramentas e dicas sobre o systemd, uma ferramenta init do Linux

http://www.h-online.com/open/features/Booting-up-Tools-and-tips-for-systemd-1570630.html

12 `journalctl`: consultar o diário do `systemd`

Quando o `systemd` substituiu os scripts init tradicionais no SUSE Linux Enterprise 12 (consulte o *Capítulo 11, O daemon* `systemd`), ele introduziu seu próprio sistema de registro denominado *diário*. Não há mais necessidade de executar um serviço baseado no `syslog`, e todos os eventos do sistema são gravados no diário.

O próprio diário é um serviço do sistema gerenciado pelo `systemd`. Seu nome completo é `systemd-journald.service`. Ele coleta e armazena dados de registro mantendo diários indexados estruturados com base nas informações de registro recebidas do kernel, de processos dos usuários, da entrada padrão e de erro dos serviços do sistema. Por padrão, o serviço `systemd-journald.service` está ativado:

```
# systemctl status systemd-journald
systemd-journald.service - Journal Service
   Loaded: loaded (/usr/lib/systemd/system/systemd-journald.service; static)
   Active: active (running) since Mon 2014-05-26 08:36:59 EDT; 3 days ago
     Docs: man:systemd-journald.service(8)
           man:journald.conf(5)
 Main PID: 413 (systemd-journal)
   Status: "Processing requests..."
   CGroup: /system.slice/systemd-journald.service
           └─413 /usr/lib/systemd/systemd-journald
[...]
```

12.1 Tornando o diário persistente

Por padrão, o diário armazena os dados de registro em `/run/log/journal/`. Como o diretório `/run/` é volátil por natureza, os dados de registro são perdidos na reinicialização. Para torná-los persistentes, deve haver um diretório `/var/log/journal/` com propriedade e permissões corretas, no qual o serviço systemd-journald pode armazenar seus dados. O `systemd` criará o diretório para você (e mudará o registro para persistente), se você fizer o seguinte:

1. Como `root`, abra o `/etc/systemd/journald.conf` para edição.

   ```
   # vi /etc/systemd/journald.conf
   ```

2. Remova o comentário da linha com `Storage=` e mude-a para

```
[...]
[Journal]
Storage=persistent
#Compress=yes
[...]
```

3. Grave o arquivo e reinicie o systemd-journald:

```
systemctl restart systemd-journald.service
```

12.2 Switches úteis do `journalctl`

Esta seção apresenta várias opções comuns úteis para melhorar o comportamento padrão do **`journalctl`**. Todos os switches estão descritos na página de manual do **`journalctl`**: **`man 1 journalctl`**.

Dica

Para mostrar todas as mensagens do diário relacionadas a determinado executável, especifique o caminho completo para o executável:

```
# journalctl /usr/lib/systemd/systemd
```

-f

Mostra apenas as mensagens mais recentes do diário e imprime novas entradas de registro à medida que são adicionadas ao diário.

-e

Imprime as mensagens e pula para o fim do diário para que as entradas mais recentes fiquem visíveis no paginador.

-r

Imprime as mensagens do diário em ordem inversa para que as entradas mais recentes sejam listadas primeiro.

-k

Mostra apenas as mensagens do kernel. Equivale à correspondência de campo `_TRANSPORT=kernel` (consulte a *Seção 12.3.3, "Filtrando com base nos campos"*).

-u

Mostra apenas as mensagens da unidade `systemd` especificada. Equivale à correspondência de campo `_SYSTEMD_UNIT=UNIDADE` (consulte a *Seção 12.3.3, "Filtrando com base nos campos"*).

```
# journalctl -u apache2
[...]
Jun 03 10:07:11 pinkiepie systemd[1]: Starting The Apache Webserver...
Jun 03 10:07:12 pinkiepie systemd[1]: Started The Apache Webserver.
```

12.3 Filtrando a saída do diário

Quando chamado sem switches, o **`journalctl`** mostra o conteúdo completo do diário, com as entradas mais antigas listadas primeiro. É possível filtrar a saída por switches e campos específicos.

12.3.1 Filtrando com base em um número de boot

O **`journalctl`** pode filtrar as mensagens com base em um boot do sistema específico. Para listar todos os boots disponíveis, execute

```
# journalctl --list-boots
-1 097ed2cd99124a2391d2cffab1b566f0 Mon 2014-05-26 08:36:56 EDT—Fri 2014-05-30
 05:33:44 EDT
 0 156019a44a774a0bb0148a92df4af81b Fri 2014-05-30 05:34:09 EDT—Fri 2014-05-30
 06:15:01 EDT
```

A primeira coluna lista a diferença de boot: `0` para o boot atual, `-1` para o anterior, `-2` para o segundo anterior, etc. A segunda coluna apresenta o ID de boot e as marcações de horário de limite da sequência de boot específica.

Mostrar todas as mensagens do boot atual:

```
# journalctl -b
```

Se você precisa ver mensagens de diário do boot anterior, adicione um parâmetro de diferença. O seguinte exemplo representa as mensagens do boot anterior:

```
# journalctl -b -1
```

Uma outra maneira é listar as mensagens de boot com base no ID de boot. Para esta finalidade, use o campo _BOOT_ID:

```
# journalctl _BOOT_ID=156019a44a774a0bb0148a92df4af81b
```

12.3.2 Filtrando com base no intervalo de tempo

É possível filtrar a saída do **journalctl** especificando a data de início e/ou de término. A especificação de data deve ser no formato "2014-06-30 9:17:16". Se a parte do horário for omitida, será considerada meia-noite. Se os segundos forem omitidos, será considerado ":00". Se a parte da data for omitida, será considerado o dia atual. Em vez da expressão numérica, é possível especificar as palavras-chave "ontem", "hoje" ou "amanhã", que se referem à meia-noite do dia anterior ao dia atual, do dia atual ou do dia posterior ao dia atual. Se você especificar "agora", vai se referir ao horário atual. É possível também especificar horários com os prefixos `-` ou `+`, que se referem aos horários antes ou depois do horário atual.

Mostrar apenas novas mensagens a partir de agora e atualizar a saída continuamente:

```
# journalctl --since "now" -f
```

Mostrar todas as mensagens desde meia-noite passada até às 3h20:

```
# journalctl --since "today" --until "3:20"
```

12.3.3 Filtrando com base nos campos

É possível filtrar a saída do diário por campos específicos. A sintaxe de um campo para correspondência é `FIELD_NAME=MATCHED_VALUE`, como `_SYSTEMD_UNIT=httpd.service`. É possível especificar várias correspondências em um única consulta para filtrar ainda mais as mensagens de saída. Consulte **`man 7 systemd.journal-fields`** para ver a lista de campos padrão.

Mostrar mensagens produzidas por um ID de processo específico:

```
# journalctl _PID=1039
```

Mostrar mensagens que pertencem a determinado ID de usuário:

```
# journalctl _UID=1000
```

Mostrar mensagens do buffer de anel do kernel (as mesmas que o **`dmesg`** produz):

```
# journalctl _TRANSPORT=kernel
```

Mostrar mensagens da saída padrão ou de erros do serviço:

```
# journalctl _TRANSPORT=stdout
```

Mostrar mensagens produzidas apenas por determinado serviço:

```
# journalctl _SYSTEMD_UNIT=avahi-daemon.service
```

Se dois campos diferentes forem especificados, apenas as entradas que corresponderem às duas expressões ao mesmo tempo serão mostradas:

```
# journalctl _SYSTEMD_UNIT=avahi-daemon.service _PID=1488
```

Se duas correspondências fizerem referência ao mesmo campo, todas as entradas correspondentes a uma das expressões serão mostradas:

```
# journalctl _SYSTEMD_UNIT=avahi-daemon.service _SYSTEMD_UNIT=dbus.service
```

É possível usar o separador "+" para combinar duas expressões em um "OR" lógico. O seguinte exemplo mostra todas as mensagens do processo do serviço Avahi com ID de processo 1480 juntamente com todas as mensagens do serviço D-Bus:

```
# journalctl _SYSTEMD_UNIT=avahi-daemon.service _PID=1480 +
 _SYSTEMD_UNIT=dbus.service
```

12.4 Investigando erros do `systemd`

Esta seção apresenta um exemplo simples que ilustra como localizar e corrigir o erro relatado pelo `systemd` durante a inicialização do **`apache2`**.

1. Tentar iniciar o serviço apache2:

   ```
   # systemctl start apache2.service
   Job for apache2.service failed. See 'systemctl status apache2.service' and
    'journalctl -xn' for details.
   ```

2. Vejamos o que diz o status do serviço:

   ```
   # systemctl status apache2.service
   apache2.service - The Apache Webserver
      Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled)
      Active: failed (Result: exit-code) since Tue 2014-06-03 11:08:13 CEST; 7min
    ago
     Process: 11026 ExecStop=/usr/sbin/start_apache2 -D SYSTEMD -DFOREGROUND \
              -k graceful-stop (code=exited, status=1/FAILURE)
   ```

   O ID do processo que causa a falha é 11026.

3. Mostrar a versão verbosa das mensagens relacionadas ao ID de processo 11026:

   ```
   # journalctl -o verbose _PID=11026
   [...]
   MESSAGE=AH00526: Syntax error on line 6 of /etc/apache2/default-server.conf:
   [...]
   ```

```
MESSAGE=Invalid command 'DocumenttRoot', perhaps misspelled or defined by a
 module
[...]
```

4. Corrigir o erro de digitação em `/etc/apache2/default-server.conf`, iniciar o serviço apache2 e imprimir seu status:

```
# systemctl start apache2 && systemctl status apache2
apache2.service - The Apache Webserver
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled)
   Active: active (running) since Tue 2014-06-03 11:26:24 CEST; 4ms ago
  Process: 11026 ExecStop=/usr/sbin/start_apache2 -D SYSTEMD -DFOREGROUND
           -k graceful-stop (code=exited, status=1/FAILURE)
 Main PID: 11263 (httpd2-prefork)
   Status: "Processing requests..."
   CGroup: /system.slice/apache2.service
           ├─11263 /usr/sbin/httpd2-prefork -f /etc/apache2/httpd.conf -D [...]
           ├─11280 /usr/sbin/httpd2-prefork -f /etc/apache2/httpd.conf -D [...]
           ├─11281 /usr/sbin/httpd2-prefork -f /etc/apache2/httpd.conf -D [...]
           ├─11282 /usr/sbin/httpd2-prefork -f /etc/apache2/httpd.conf -D [...]
           ├─11283 /usr/sbin/httpd2-prefork -f /etc/apache2/httpd.conf -D [...]
           └─11285 /usr/sbin/httpd2-prefork -f /etc/apache2/httpd.conf -D
 [...]
```

12.5 Configuração do journald

É possível ajustar o comportamento do serviço systemd-journald modificando `/etc/systemd/journald.conf`. Esta seção apresenta apenas as configurações de opção básicas. Para ver a descrição completa do arquivo, consulte **`man 5 journald.conf`**. Observe que é necessário reiniciar o diário para que as mudanças entrem em vigor com

```
# systemctl restart systemd-journald.service
```

12.5.1 Mudando o limite de tamanho do diário

Se os dados do registro em diário forem gravados em um local persistente (consulte a *Seção 12.1, "Tornando o diário persistente"*), eles usarão até 10% do sistema de arquivos no qual o `/var/log/journal` reside. Por exemplo, se `/var/log/journal` estiver em uma partição `/var` de 30 GB, o diário poderá usar até 3 GB de espaço em disco. Para mudar esse limite, altere (e remova o comentário) a opção `SystemMaxUse`:

```
SystemMaxUse=50M
```

12.5.2 Encaminhando o diário para `/dev/ttyX`

É possível encaminhar o diário para um dispositivo de terminal para você receber informações sobre mensagens do sistema na tela de terminal de sua preferência, por exemplo `/dev/tty12`. Mude as seguintes opções de journald para

```
ForwardToConsole=yes
TTYPath=/dev/tty12
```

12.5.3 Encaminhando o diário para o recurso do syslog

O Journald é retroativamente compatível com as implementações tradicionais do syslog, como `rsyslog`. Verifique se as afirmativas a seguir são válidas:

- O rsyslog está instalado.

  ```
  # rpm -q rsyslog
  rsyslog-7.4.8-2.16.x86_64
  ```

- O serviço rsyslog está habilitado.

  ```
  # systemctl is-enabled rsyslog.service
  enabled
  ```

- O encaminhamento para syslog está habilitado em `/etc/systemd/journald.conf`.

  ```
  ForwardToSyslog=yes
  ```

13 O carregador de boot GRUB 2

Este capítulo descreve como configurar o GRUB 2, o carregador de boot usado no SUSE® Linux Enterprise Desktop. Ele é o sucessor do carregador de boot tradicional GRUB, agora chamado de "GRUB 2 Legacy". O GRUB 2 tornou-se o carregador de boot padrão do SUSE® Linux Enterprise Desktop desde a versão 12. Um módulo do YaST está disponível para definir as configurações mais importantes. O procedimento de boot como um todo é detalhado no *Capítulo 10, Inicializando um sistema Linux*. Para obter detalhes sobre o suporte a Boot Seguro para máquinas UEFI, consulte o *Capítulo 14, UEFI (Unified Extensible Firmware Interface)*.

13.1 Principais diferenças entre o GRUB Legacy e o GRUB 2

- A configuração é armazenada em arquivos diferentes.
- Mais sistemas de arquivos são suportados (por exemplo, Btrfs).
- Pode ler arquivos armazenados em dispositivos LVM ou RAID diretamente.
- A interface do usuário pode ser traduzida e alterada com temas.
- Inclui um mecanismo para carregar módulos que suportam recursos adicionais, como sistemas de arquivos, etc.
- Pesquisa e gera automaticamente entradas de boot para outros kernels e sistemas operacionais, como o Windows.
- Inclui um console mínimo do tipo Bash.

13.2 Estrutura do arquivo de configuração

A configuração do GRUB 2 baseia-se nos seguintes arquivos:

`/boot/grub2/grub.cfg`

Este arquivo inclui a configuração dos itens de menu do GRUB 2. Ele substitui o `menu.lst` usado no GRUB Legacy. O `grub.cfg` é automaticamente gerado pelo comando **`grub2-mkconfig`** e não deve ser editado.

`/boot/grub2/custom.cfg`

Este arquivo opcional é diretamente originado pelo `grub.cfg` no momento da inicialização e pode ser usado para adicionar itens personalizados ao menu de boot.

`/etc/default/grub`

Este arquivo controla as configurações do usuário do GRUB 2 e, normalmente, inclui outras configurações de ambiente, como fundos e temas.

Scripts em `/etc/grub.d/`

Os scripts neste diretório são lidos durante a execução do comando **`grub2-mkconfig`** . Suas instruções estão integradas ao arquivo de configuração principal `/boot/grub/grub.cfg`.

`/etc/sysconfig/bootloader`

Este arquivo de configuração é usado ao configurar o carregador de boot com o YaST e sempre que um novo kernel é instalado. Ele é avaliado pelo perl-bootloader, que modifica o arquivo de configuração do carregador de boot apropriadamente (por exemplo, `/boot/grub2/grub.cfg` para o GRUB 2). O `/etc/sysconfig/bootloader` não é um arquivo de configuração específico do GRUB 2, os valores são aplicados a qualquer carregador de boot instalado no SUSE Linux Enterprise Desktop.

`/boot/grub2/x86_64-efi, ,`

Estes arquivos de configuração incluem opções específicas da arquitetura.

O GRUB 2 pode ser controlado de várias maneiras. As entradas de boot de uma configuração existente podem ser selecionadas no menu gráfico (splash screen). A configuração é carregada do arquivo `/boot/grub2/grub.cfg`, que é compilado de outros arquivos de configuração (veja abaixo). Todos os arquivos de configuração do GRUB 2 são considerados arquivos do sistema, e você precisa de privilégios de `root` para editá-los.

Nota: Ativando mudanças de configuração

Depois de editar manualmente os arquivos de configuração do GRUB 2, você deverá executar **`grub2-mkconfig`** para ativar as mudanças. Porém, isso não é necessário ao mudar a configuração com o YaST, já que ele executa **`grub2-mkconfig`** automaticamente.

13.2.1 O arquivo /boot/grub2/grub.cfg

A splash screen gráfica com o menu de boot baseia-se no arquivo de configuração do GRUB 2 `/boot/grub2/grub.cfg`, que contém as informações sobre todas as partições ou sistemas operacionais que podem ser inicializados pelo menu.

Todas as vezes em que o sistema é inicializado, o GRUB 2 carrega o arquivo de menu diretamente do sistema de arquivos. Por esta razão, o GRUB 2 não precisa ser reinstalado após as modificações no arquivo de configuração. O `grub.cfg` é recriado automaticamente com as instalações ou remoções do kernel.

O `grub.cfg` é compilado pelo **`grub2-mkconfig`** do arquivo `/etc/default/grub` e dos scripts que estão no diretório `/etc/grub.d/`. Portanto, você nunca deve editar o arquivo manualmente. Em vez disso, edite os arquivos de origem relacionados ou use o módulo *Carregador de Boot* do YaST para modificar a configuração, conforme descrito na *Seção 13.3, "Configurando o carregador de boot com o YaST"*.

13.2.2 O arquivo /etc/default/grub

Há mais opções gerais do GRUB 2 aqui, como o horário em que o menu é exibido ou o OS padrão para inicializar. Para listar todas as opções disponíveis, consulte a saída do seguinte comando:

```
grep "export GRUB_DEFAULT" -A50 /usr/sbin/grub2-mkconfig | grep GRUB_
```

Além das variáveis já definidas, o usuário pode incluir suas próprias variáveis e usá-las posteriormente nos scripts que estão no diretório `/etc/grub.d`.

Após editar o `/etc/default/grub`, execute **`grub2-mkconfig`** para atualizar o arquivo de configuração principal.

Nota: Escopo

Todas as opções definidas neste arquivo são opções gerais que afetam todas as entradas de boot. É possível definir opções específicas para os Kernels ou o hipervisor do Xen usando as opções de configuração GRUB_*_XEN_*. Veja os detalhes a seguir.

`GRUB_DEFAULT`

Define a entrada do menu de boot que será inicializada por padrão. Seu valor pode ser numérico, o nome completo de uma entrada do menu ou "saved" (gravado).

`GRUB_DEFAULT=2` inicializa a terceira entrada (contada a partir de zero) do menu de boot. `GRUB_DEFAULT="2>0"` inicializa a primeira entrada do submenu da terceira entrada do menu de nível superior.

`GRUB_DEFAULT="Exemplo de entrada do menu de boot"` inicializa a entrada do menu com o título “Exemplo de entrada do menu de boot”.

`GRUB_DEFAULT=saved` inicializa a entrada especificada pelos comandos **`grub2-reboot`** ou **`grub2-set-default`** . Enquanto **`grub2-reboot`** define a entrada de boot padrão apenas para a próxima reinicialização, o **`grub2-set-default`** define a entrada de boot padrão até ser modificada.

`GRUB_HIDDEN_TIMEOUT`

Aguarda o usuário pressionar uma tecla durante o número especificado de segundos. Durante o período, nenhum menu é exibido, exceto se o usuário pressionar uma tecla. Se nenhuma tecla for pressionada durante o período especificado, o controle será passado para `GRUB_TIMEOUT`. `GRUB_HIDDEN_TIMEOUT=0` verifica primeiro se a tecla `Shift` foi pressionada e mostra o menu de boot em caso afirmativo, do contrário, inicializa a entrada do menu padrão imediatamente. Este é o procedimento padrão quando somente um OS inicializável é identificado pelo GRUB 2.

`GRUB_HIDDEN_TIMEOUT_QUIET`

Se `false` (falso) for especificado, um temporizador de contagem regressiva será exibido em uma tela em branco quando o recurso `GRUB_HIDDEN_TIMEOUT` estiver ativo.

`GRUB_TIMEOUT`

O período em segundos durante o qual o menu de boot é exibido antes de inicializar a entrada de boot padrão automaticamente. Se você pressionar uma tecla, o tempo de espera será cancelado, e o GRUB 2 vai aguardar até você fazer uma seleção manualmente. `GRUB_TIMEOUT=-1` exibe o menu até você selecionar a entrada de boot manualmente.

`GRUB_CMDLINE_LINUX`

As entradas nesta linha são adicionadas ao fim das entradas de boot para o modo normal e de recuperação. Use-a para adicionar parâmetros do kernel à entrada de boot.

`GRUB_CMDLINE_LINUX_DEFAULT`

Igual a `GRUB_CMDLINE_LINUX`, mas as entradas são anexadas apenas no modo normal.

`GRUB_CMDLINE_LINUX_RECOVERY`

Igual a `GRUB_CMDLINE_LINUX`, mas as entradas são anexadas apenas no modo de recuperação.

`GRUB_CMDLINE_LINUX_XEN_REPLACE`

Esta entrada substitui completamente os parâmetros de `GRUB_CMDLINE_LINUX` por todas as entradas de boot do Xen.

`GRUB_CMDLINE_LINUX_XEN_REPLACE_DEFAULT`

Igual a `GRUB_CMDLINE_LINUX_XEN_REPLACE`, mas substitui apenas os parâmetros de `GRUB_CMDLINE_LINUX_DEFAULT`.

`GRUB_CMDLINE_XEN`

Esta entrada especifica os parâmetros de kernel apenas para o kernel convidado do Xen. O princípio da operação é o mesmo de `GRUB_CMDLINE_LINUX`.

`GRUB_CMDLINE_XEN_DEFAULT`

Igual a `GRUB_CMDLINE_XEN`. O princípio da operação é o mesmo de `GRUB_CMDLINE_LINUX_DEFAULT`.

`GRUB_TERMINAL`

Habilita e especifica um dispositivo de terminal de entrada/saída. Pode ser `console` (consoles BIOS e EFI do PC), `serial` (terminal serial), `ofconsole` (console do Open Firmware) ou o `gfxterm` padrão (saída do modo gráfico). É possível também habilitar mais de um dispositivo colocando as opções necessárias entre aspas, por exemplo, `GRUB_TERMINAL="console serial"`.

`GRUB_GFXMODE`

A resolução usada para o terminal gráfico `gfxterm` . Observe que você só pode usar os modos suportados por sua placa gráfica (VBE). O padrão é "auto", que tenta selecionar uma resolução preferencial. É possível mostrar as resoluções de tela disponíveis para o GRUB 2 digitando **`vbeinfo`** na linha de comando do GRUB 2. Para acessar a linha de comando, digite c quando aparecer a tela do menu de boot do GRUB 2.

É possível também especificar a profundidade de cores anexando-a à configuração da resolução, por exemplo, `GRUB_GFXMODE=1280x1024x24`.

`GRUB_BACKGROUND`

Defina uma imagem de fundo para o terminal gráfico `gfxterm`. A imagem deve ser um arquivo legível pelo GRUB 2 no momento da inicialização, que deve terminar com o sufixo `.png`, `.tga`, `.jpg` ou `.jpeg`. Se necessário, a imagem será dimensionada para caber na tela.

`GRUB_DISABLE_OS_PROBER`

Se esta opção for definida como `true` (verdadeiro), a pesquisa automática de outros sistemas operacionais será desabilitada. Apenas as imagens do kernel em `/boot/` e as opções de seus próprios scripts em `/etc/grub.d/` serão detectadas.

`SUSE_BTRFS_SNAPSHOT_BOOTING`

Se esta opção for definida como `true` (verdadeiro), o GRUB 2 poderá ser inicializado diretamente nos instantâneos do Snapper. Para obter mais informações, leia a *Seção 4.3, "Rollback do sistema por inicialização de instantâneos"*.

Nota

Todos os parâmetros `*_DEFAULT` podem ser controlados manualmente ou pelo YaST.

Para ver a lista completa de opções, consulte o manual do GNU GRUB (http://www.gnu.org/software/grub/manual/grub.html#Simple-configuration). Para ver a lista completa de parâmetros possíveis, visite http://en.opensuse.org/Linuxrc.

13.2.3 Scripts em `/etc/grub.d`

Os scripts neste diretório são lidos durante a execução do comando **`grub2-mkconfig`** , e suas instruções estão incorporadas ao `/boot/grub2/grub.cfg`. A ordem dos itens de menu no `grub.cfg` é determinada pela ordem em que os arquivos são executados nesse diretório. Os arquivos com um número à esquerda são executados primeiro, começando pelo número mais baixo. `00_header` é executado antes de `10_linux`, que é executado antes de `40_custom`. Se houver arquivos com nomes alfabéticos, eles serão executados depois dos arquivos com números nos nomes. Apenas os arquivos executáveis geram uma saída para `grub.cfg` durante a execução de **`grub2-mkconfig`**. Por padrão, todos os arquivos no diretório `/etc/grub.d` são executáveis. Os scripts mais importantes são:

`00_header`

Define variáveis de sistema, como locais de arquivos do sistema, configurações de tela, temas e entradas que já foram gravadas. Ele também importa as preferências armazenadas no `/etc/default/grub`. Normalmente, não é necessário modificar este arquivo.

`10_linux`

Identifica os kernels do Linux no dispositivo raiz e cria entradas de menu relevantes. Inclui a opção de modo de recuperação associada, se habilitada. Somente o kernel mais recente é exibido na página de menu principal, com kernels adicionais incluídos em um submenu.

`30_os-prober`

Este script usa o **`OS-prober`** para procurar o Linux e outros sistemas operacionais e apresenta os resultados no menu do GRUB 2. Há seções para identificar outros sistemas operacionais específicos, como Windows ou OS X.

`40_custom`

Este arquivo oferece uma forma simples de incluir entradas de boot personalizadas no `grub.cfg`. Lembre-se de que você não muda a parte `exec tail -n +3 $0` que fica no começo.

`90_persistent`

Este é um script especial que copia uma parte correspondente do arquivo `grub.cfg` e retorna sua saída inalterada. Desta forma, é possível modificar essa parte do `grub.cfg` diretamente, e a mudança se mantém após a execução de **`grub2-mkconfig`** .

A sequência de processamento é definida pelos números precedentes, sendo o menor número executado primeiro. Se os scripts forem precedidos pelo mesmo número, a ordem alfabética do nome completo determinará a disposição.

13.2.4 Mapeamento entre unidades BIOS e dispositivos Linux

No GRUB Legacy, o arquivo de configuração `device.map` era usado para derivar nomes de dispositivos Linux dos números das unidades BIOS. O mapeamento entre as unidades BIOS e os dispositivos Linux nem sempre pode ser previsto corretamente. Por exemplo, o GRUB Legacy obterá a ordem incorreta se a sequência de boot das unidades IDE e SCSI for trocada na configuração do BIOS.

O GRUB 2 evita este problema usando strings de ID de dispositivo (UUIDs) ou rótulos de sistema de arquivos ao gerar o `grub.cfg`. Os utilitários do GRUB 2 criam um mapa de dispositivos temporário simultaneamente, que, na maioria das vezes, é suficiente, sobretudo no caso de sistemas de disco único.

Mas se você tiver que anular o mecanismo de mapeamento de dispositivos automático do GRUB 2, crie seu próprio arquivo de mapeamento `/boot/grub2/device.map`. O seguinte exemplo muda o mapeamento para transformar o `DISK 3` no disco de boot. Observe que os números de partição do GRUB 2 começam com `1`, e não com `0` como no GRUB Legacy.

```
(hd1)  /dev/disk-by-id/DISK3 ID
(hd2)  /dev/disk-by-id/DISK1 ID
(hd3)  /dev/disk-by-id/DISK2 ID
```

13.2.5 Editando as entradas de menu durante o procedimento de boot

É útil editar diretamente as entradas de menu quando o sistema não é mais inicializado por causa de falha na configuração. Ele também pode ser usado para testar novas configurações sem alterar a configuração do sistema.

1. No menu gráfico de boot, selecione a entrada que deseja editar com as teclas de seta.
2. Pressione E para abrir o editor baseado em texto.
3. Use as teclas de seta para ir até a linha que deseja editar.

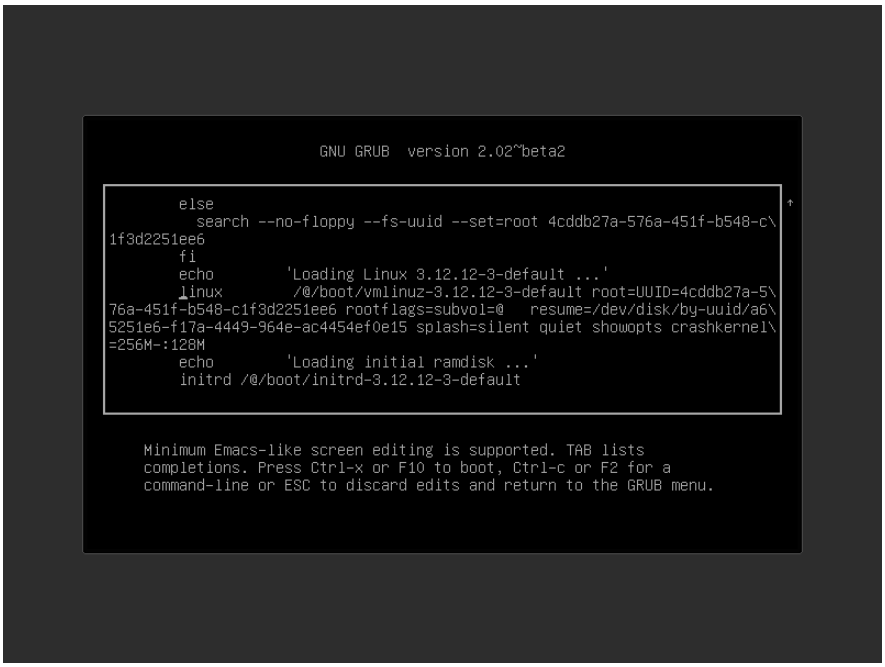

GNU GRUB version 2.02~beta2
else
search --no-floppy --fs-uuid --set=root 4cddb27a-576a-451f-b548-c\
1f3d2251ee6
fi
echo 'Loading Linux 3.12.12-3-default ...'
linux /@/boot/vmlinuz-3.12.12-3-default root=UUID=4cddb27a-5\
76a-451f-b548-c1f3d2251ee6 rootflags=subvol=@ resume=/dev/disk/by-uuid/a6\
5251e6-f17a-4449-964e-ac4454ef0e15 splash=silent quiet showopts crashkernel\
=256M-:128M
echo 'Loading initial ramdisk ...'
initrd /@/boot/initrd-3.12.12-3-default
Minimum Emacs-like screen editing is supported. TAB lists
completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a
command-line or ESC to discard edits and return to the GRUB menu.

FIGURA 13.1 EDITOR DE BOOT DO GRUB 2

Agora você tem duas opções:

a. Adicione parâmetros separados por espaço ao fim da linha que começa com `linux` ou `linuxefi` para editar os parâmetros de kernel. Há uma lista completa de parâmetros disponível em http://en.opensuse.org/Linuxrc.

b. Se preferir, edite as opções gerais para mudar a versão do kernel, por exemplo. A tecla `→|` sugere todas as complementações possíveis.

4. Pressione `F10` para inicializar o sistema com as mudanças feitas ou pressione `Esc` para descartar suas edições e retornar ao menu do GRUB 2.

As mudanças feitas desta maneira só se aplicam ao processo de boot atual, elas não são gravadas permanentemente.

Importante: layout do teclado durante o procedimento de boot

O layout do teclado norte-americano é o único disponível na hora de inicializar. Consulte a *Figura 30.2, "Layout do teclado dos EUA"*.

Nota: Carregador de boot na mídia de instalação

O Carregador de Boot da mídia de instalação em sistemas com BIOS tradicional ainda é o GRUB Legacy. Para adicionar opções de boot, selecione uma entrada e comece a digitar. As adições feitas à entrada de boot de instalação são gravadas no sistema instalado permanentemente.

13.2.6 Configurando uma senha de boot

Mesmo antes da inicialização do sistema operacional, o GRUB 2 permite acesso aos sistemas de arquivos. Os usuários que não têm permissões de root poderão acessar os arquivos no sistema Linux aos quais não têm acesso depois que o sistema for inicializado. Para bloquear esse tipo de acesso ou impedir que os usuários inicializem determinadas entradas de menu, defina uma senha de boot.

Importante:

Se definida, a senha de boot será necessária em cada inicialização, o que significa que o sistema não será inicializado automaticamente.

Para definir uma senha de boot, faça o seguinte. Se preferir, use o YaST (*Proteger Carregador de Boot com Senha*).

1. Criptografe a senha usando **`grub2-mkpasswd-pbkdf2:`**

```
tux >  sudo grub2-mkpasswd-pbkdf2
Password: ****
Reenter password: ****
PBKDF2 hash of your password is grub.pbkdf2.sha512.10000.9CA4611006FE96BC77A...
```

2. Cole a string resultante no arquivo `/etc/grub.d/40_custom` juntamente com o comando **`set superusers`**.

```
set superusers="root"
password_pbkdf2 root grub.pbkdf2.sha512.10000.9CA4611006FE96BC77A...
```

3. Execute `grub2-mkconfig` para importar as mudanças para o arquivo de configuração principal.

   Após a reinicialização, você terá que informar o nome de usuário e a senha ao tentar inicializar uma entrada de menu. Insira `root` e a senha digitada durante o comando `grub2-mkpasswd-pbkdf2`. Se as credenciais estiverem corretas, o sistema inicializará a entrada de boot selecionada.

13.3 Configurando o carregador de boot com o YaST

O modo mais fácil de configurar opções gerais do carregador de boot no sistema SUSE Linux Enterprise Desktop é usar o módulo do YaST. No *Centro de Controle do YaST*, selecione *Sistema* › *Carregador de Boot*. O módulo mostra a configuração do carregador de boot atual do sistema e permite fazer mudanças.

Use a guia *Opções de Código de Boot* para ver e mudar configurações relativas a tipo, local e definições avançadas do carregador. Para usar o carregador de boot GRUB 2, verifique se ele está selecionado na lista de carregadores de boot disponíveis.

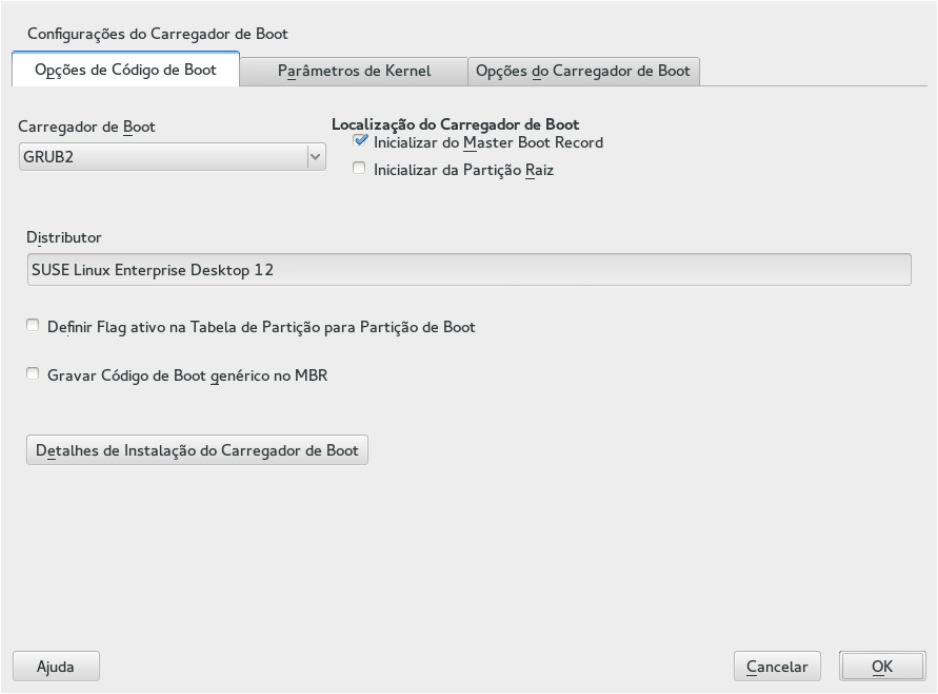

Configurações do Carregador de Boot
Opções de Código de Boot
Parâmetros de Kernel
Opções do Carregador de Boot
Carregador de Boot
GRUB2
Localização do Carregador de Boot
Inicializar do Master Boot Record
Inicializar da Partição Raiz
Distributor
SUSE Linux Enterprise Desktop 12
Definir Flag ativo na Tabela de Partição para Partição de Boot
Gravar Código de Boot genérico no MBR
Detalhes de Instalação do Carregador de Boot
Ajuda
Cancelar
OK

FIGURA 13.2 PARÂMETROS DE KERNEL

13.3.1 Mudando o tipo de carregador de boot

Defina o tipo de carregador de boot na guia *Opções de Código de Boot*. O carregador de boot padrão no SUSE Linux Enterprise Desktop é o GRUB 2. Para usar o GRUB ou o GRUB2-EFI, faça o seguinte:

PROCEDIMENTO 13.1 MUDANDO O TIPO DE CARREGADOR DE BOOT

1. Em *Carregador de Boot*, selecione *GRUB2*, *GRUB2-EFI* ou uma das outras entradas.

   Importante: Sistemas EFI exigem GRUB2-EFI

   Se você tem um sistema EFI, é possível instalar apenas o GRUB2-EFI, senão o sistema não poderá mais ser inicializado.

2. Na caixa de diálogo aberta, selecione uma das seguintes ações:

   Propor Nova Configuração
   : Faça com que o YaST proponha uma nova configuração.

   Converter Configuração Atual
   : Faça com que o YaST converta a configuração atual. Na conversão da configuração, algumas definições podem ser perdidas.

   Iniciar Nova Configuração do Início
   : Grave uma configuração personalizada. Esta ação não está disponível durante a instalação do SUSE Linux Enterprise Desktop.

   Ler Configuração Gravada em Disco
   : Carregue seu próprio arquivo de configuração do carregador de boot. Esta ação não está disponível durante a instalação do SUSE Linux Enterprise Desktop.

3. Clique em *OK* duas vezes para gravar as mudanças.

Durante a conversão, a antiga configuração do GRUB 2 é gravada no disco. Para usá-la, basta voltar o tipo de carregador de boot para GRUB 2 e escolher *Recuperar Configuração Salva antes da Conversão*. Esta ação fica disponível somente em um sistema instalado.

Nota: carregador de boot personalizado

Para usar um carregador de boot diferente dos que estão na lista, selecione *Não Instalar Nenhum Carregador de Boot*. Leia a documentação do seu carregador de boot cuidadosamente antes de escolher esta opção.

13.3.2 Modificando a localização do carregador de boot

Para modificar o local do carregador de boot, siga estas etapas:

PROCEDIMENTO 13.2 MUDANDO A LOCALIZAÇÃO DO CARREGADOR DE BOOT

1. Selecione a guia *Opções de Código de Boot* e escolha uma das seguintes opções para *Localização do Carregador de Boot*:

   Boot do Master Boot Record

   Instala o carregador de boot no MBR do primeiro disco (de acordo com a sequência de boot predefinida no BIOS).

   Boot da partição raiz

   Instala o carregador de boot no setor de boot da partição `/` (padrão).

   Boot da partição de boot

   Instala o carregador de boot no setor de boot da partição `/boot`.

   Boot da partição estendida

   Instala o carregador de boot no container da partição estendida.

   Partição de boot personalizada

   Use esta opção para especificar a localização do carregador de boot manualmente.

2. Clique em *OK* para aplicar as mudanças.

13.3.3 Ajustando a ordem dos discos

Se o computador tiver mais do que um disco rígido, você poderá especificar a sequência de boot dos discos. Para obter mais informações, consulte a *Seção 13.2.4, "Mapeamento entre unidades BIOS e dispositivos Linux"*.

PROCEDIMENTO 13.3 DEFININDO A ORDEM DOS DISCOS

1. Abra a guia *Opções de Código de Boot*.
2. Clique em *Detalhes de Instalação do Carregador de Boot*.
3. Se mais de um disco for listado, selecione um disco e clique em *Para cima* ou *Para baixo* para reordenar os discos exibidos.
4. Clique em *OK* duas vezes para gravar as mudanças.

13.3.4 Configurando as opções avançadas

As opções avançadas de boot podem ser configuradas por meio de *Instalação do Carregador de Boot* › *Opções do Carregador de Boot*.

13.3.4.1 Guia 1: *Opções do Carregador de Boot*

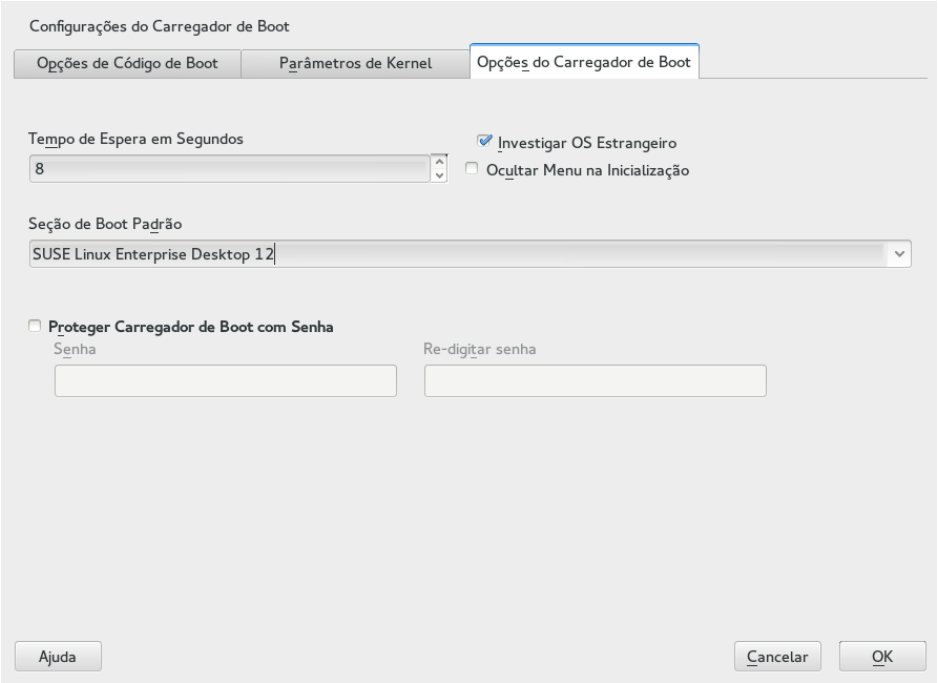


FIGURA 13.3 OPÇÕES DO CARREGADOR DE BOOT

Tempo de espera do carregador de boot

Mude o valor de *Tempo de Espera em Segundos* digitando um novo valor e clicando na tecla de seta apropriada com o mouse.

Investigar OS Estrangeiro

Quando selecionada, o carregador de boot procura por outros sistemas, como Windows ou outras instalações do Linux.

Ocultar Menu na Inicialização

Oculta o menu de boot e a entrada padrão.

Ajustando a entrada de boot padrão

Selecione a entrada desejada na lista “Seção de Boot Padrão”. Observe que o sinal de “>” no nome da entrada de boot delimita a seção de boot e sua subseção.

Proteger Carregador de Boot com Senha

Protege o carregador de boot e o sistema com uma senha adicional. Para obter mais detalhes, consulte a *Seção 13.2.6, “Configurando uma senha de boot”*.

13.3.4.2 Guia 2: *Parâmetros de Kernel*

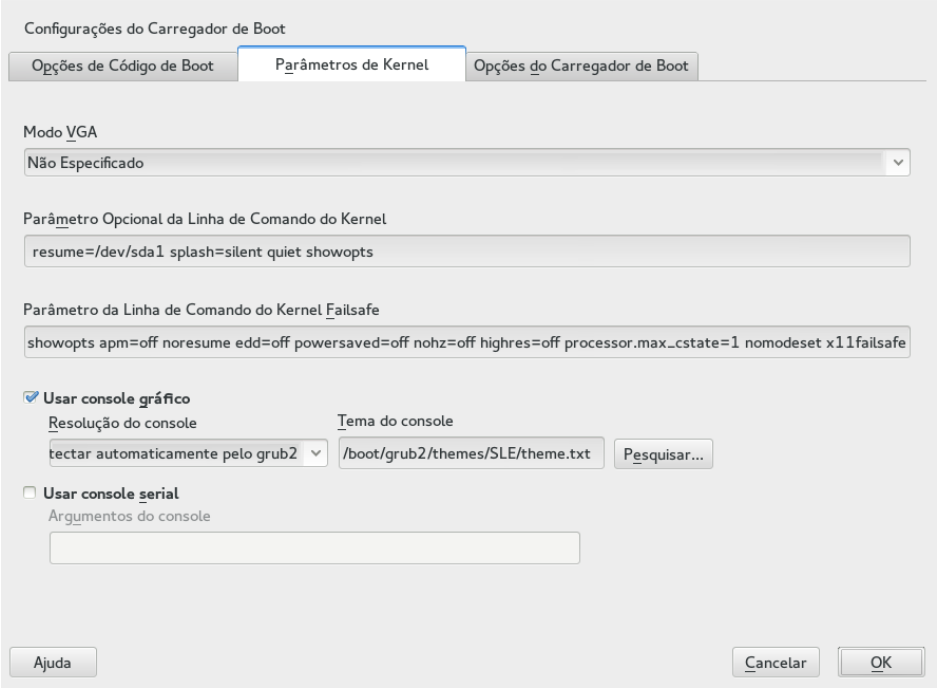


FIGURA 13.4 PARÂMETROS DE KERNEL

Modo VGA

A opção Modo VGA especifica a resolução de tela padrão durante o processo de boot.

Parâmetro Opcional da Linha de Comando do Kernel

Os Parâmetros de Kernel são adicionados ao fim dos parâmetros padrão. Os Parâmetros Opcionais apenas são adicionados ao kernel normal, e os parâmetros fail-safe (à prova de falhas) são adicionados somente ao kernel fail-safe ou de recuperação. Para ver a lista de todos os parâmetros possíveis, visite http://en.opensuse.org/Linuxrc.

Usar console gráfico

Quando marcada, o menu de boot aparece na splash screen gráfica, e não em modo de texto. A resolução da tela de boot pode ser definida na lista *Resolução do console*, e o arquivo de definição de tema gráfico pode ser especificado com o seletor de arquivos do *Tema do console*.

Usar o Console Serial

Se a sua máquina é controlada por um console serial, ative essa opção e especifique a porta COM que será usada e em qual velocidade. Consulte **`info grub`** ou o site http://www.gnu.org/software/grub/manual/grub.html#Serial-terminal

13.3.4.3 Guia 3: *Opções de Código de Boot*

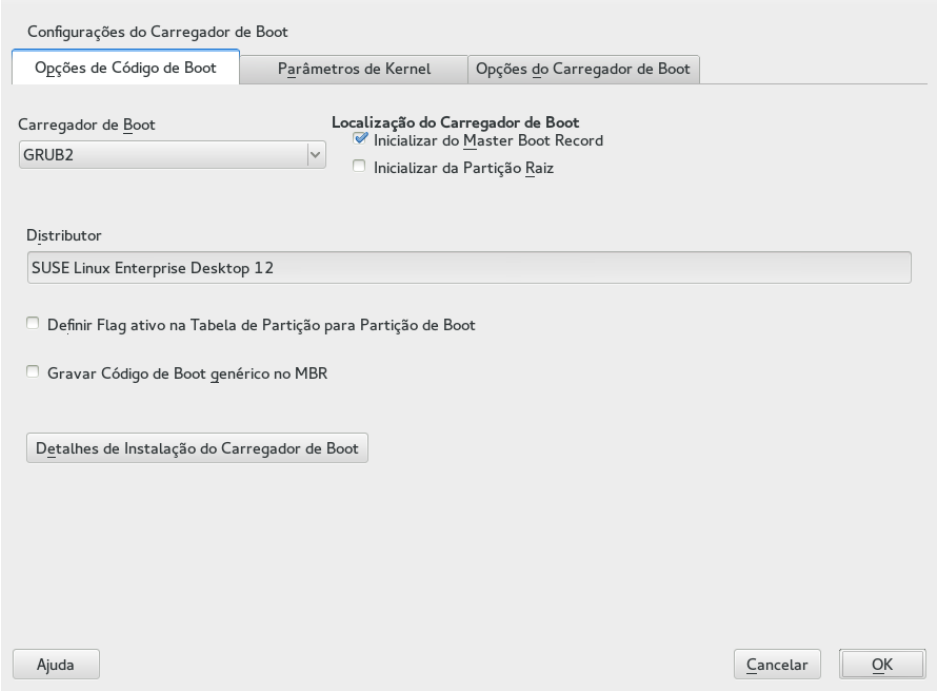

Configurações do Carregador de Boot
Opções de Código de Boot
Parâmetros de Kernel
Opções do Carregador de Boot
Carregador de Boot
GRUB2
Localização do Carregador de Boot
Inicializar do Master Boot Record
Inicializar da Partição Raiz
Distributor
SUSE Linux Enterprise Desktop 12
Definir Flag ativo na Tabela de Partição para Partição de Boot
Gravar Código de Boot genérico no MBR
Detalhes de Instalação do Carregador de Boot
Ajuda
Cancelar
OK

FIGURA 13.5 PARÂMETROS DE KERNEL

Definir Flag Ativo na Tabela de Partição para a Partição de Boot

Ativa a partição que contém o carregador de boot. Alguns sistemas operacionais legados (como o Windows) podem ser inicializados apenas de uma partição ativa.

Gravar Código de Boot Genérico no MBR

Substitui o MBR atual por um código genérico independente de sistema operacional.

13.4 Diferenças no uso de terminais no System z

Nos terminais 3215 e 3270, há algumas diferenças e limitações referentes à maneira de mover o cursor e emitir comandos de edição no GRUB 2.

13.4.1 Limitações

Interatividade

A interatividade é altamente limitada. A digitação quase sempre não resulta em feedback visual. Para ver onde está o cursor, digite um sublinhado (_).

Nota

O terminal 3270 é muito melhor no que diz respeito à exibição e atualização de telas do que o terminal 3215.

Movimento do Cursor

O movimento do cursor "tradicional" não é possível. Alt, Meta, Ctrl e as teclas de cursor não funcionam. Para mover o cursor, use as combinações de teclas listadas na *Seção 13.4.2, "Combinações de tecla"*.

Acento Circunflexo

O acento circunflexo (^) é usado como caractere de controle. Para digitar um ^ literal seguido de uma letra, digite ^, ^, *LETRA*.

Digite

A tecla Enter não funciona; em vez disso, use ^–j.

13.4.2 Combinações de tecla

Substitutos Comuns:	^ J	acionar (“Enter”)
	^ L	interromper, retornar ao “estado” anterior
	^ I	preenchimento de tabulação (nos modos de edição e shell)
Teclas Disponíveis no Modo de Menu:	^ A	primeira entrada
	^ E	última entrada
	^ P	entrada anterior
	^ N	próxima entrada
	^ G	página anterior
	^ C	próxima página
	^ F	inicializar entrada selecionada ou inserir submenu (igual a ^ J)
	E	editar entrada selecionada
	c	inserir GRUB-Shell
Teclas Disponíveis no Modo de Edição:	^ P	linha anterior
	^ N	próxima linha
	^ B	caractere de recuo
	^ F	caractere de avanço
	^ A	começo da linha
	^ E	fim da linha

	^ H	backspace
	^ D	apagar
	^ K	eliminar linha
	^ Y	remover
	^ O	abrir linha
	^ L	atualizar tela
	^ X	inicializar entrada
	^ C	inserir GRUB-Shell
Teclas Disponíveis no Modo de Linha de Comando:	^ P	comando anterior
	^ N	próximo comando do histórico
	^ A	começo da linha
	^ E	fim da linha
	^ B	caractere de recuo
	^ F	caractere de avanço
	^ H	backspace
	^ D	apagar
	^ K	eliminar linha
	^ U	descartar linha
	^ Y	remover

13.5 Comandos úteis do GRUB 2

`grub2-mkconfig`

Gera um novo `/boot/grub2/grub.cfg` com base no `/etc/default/grub` e nos scripts de `/etc/grub.d/`.

EXEMPLO 13.1 USO DO GRUB2-MKCONFIG

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

Dica: Verificação de sintaxe

A execução de **`grub2-mkconfig`** sem nenhum parâmetro imprime a configuração em STDOUT, de onde é possível revisá-la. Use **`grub2-script-check`** após a gravação de `/boot/grub2/grub.cfg` para verificar sua sintaxe.

`grub2-mkrescue`

Cria uma imagem de recuperação inicializável da configuração do GRUB 2 instalado.

EXEMPLO 13.2 USO DO GRUB2-MKRESCUE

```
grub2-mkrescue -o save_path/name.iso iso
```

`grub2-script-check`

Verifica se há erros de sintaxe no arquivo especificado.

EXEMPLO 13.3 USO DO GRUB2-SCRIPT-CHECK

```
grub2-check-config /boot/grub2/grub.cfg
```

`grub2-once`

Defina a entrada de boot padrão apenas para a próxima inicialização. Para ver a lista de entradas de boot disponíveis, use a opção `--list`.

EXEMPLO 13.4 USO DO GRUB2-ONCE

```
grub2-once number_of_the_boot_entry
```

Dica

Chame o programa sem nenhuma opção para obter a lista completa de todas as opções possíveis.

13.6 Mais informações

Em http://www.gnu.org/software/grub/, há informações abrangentes sobre o GRUB 2. Consulte também a página de informações **grub**. Você também pode pesquisar a palavra-chave “GRUB 2” na Pesquisa de Informações Técnicas em http://www.suse.com/support para obter informações sobre problemas específicos.

14 UEFI (Unified Extensible Firmware Interface)

UEFI (Unified Extensible Firmware Interface) é a interface entre o firmware que vem com o hardware do sistema, todos os componentes do hardware do sistema e o sistema operacional.

A UEFI está se tornando cada vez mais disponível em sistemas PC e substituindo o PC-BIOS tradicional. Por exemplo, a UEFI suporta apropriadamente sistemas de 64 bits e oferece inicialização segura (“Boot Seguro”, firmware versão 2.3.1c ou superior necessário), que é um dos recursos mais importantes. Por fim, com a UEFI, um firmware padrão estará disponível em todas as plataformas x86.

A UEFI oferece também as seguintes vantagens:

- Inicialização de discos grandes (mais de 2 TiB) com GPT (Tabela de Partição GUID).
- Drivers e arquitetura independente da CPU.
- Ambiente pré-OS flexível com recursos de rede.
- CSM (Módulo de Suporte de Compatibilidade) para suportar inicialização de sistemas operacionais legados por emulação do tipo PC-BIOS.

Para obter mais informações, consulte http://en.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface. As seguintes seções não são uma visão geral da UEFI, são apenas dicas sobre como alguns recursos são implementados no SUSE Linux Enterprise.

14.1 Boot seguro

Para a UEFI, proteger o processo de boot significa estabelecer uma cadeia de confiança. A “plataforma” é a raiz da cadeia de confiança; no contexto do SUSE Linux Enterprise, a placa-mãe e o firmware on-board podem ser considerados a “plataforma”. Explicando de uma maneira um pouco diferente, imagine o fornecedor do hardware e a cadeia de confiança que parte desse fornecedor para os fabricantes dos componentes, os fornecedores de OS, etc.

A confiança é expressada através da criptografia de chave pública. O fornecedor do hardware coloca a chamada PK (Chave de Plataforma) no firmware, representando a base da confiança. A relação de confiança com os fornecedores do sistema operacional e os outros é documentada pela assinatura das chaves usando a Chave de Plataforma.

Por fim, a segurança é estabelecida exigindo que nenhum código seja executado pelo firmware, exceto se tiver sido assinado por uma das chaves “confiáveis”, seja um carregador de boot de OS, algum driver localizado na memória flash de uma placa PCI Express ou no disco, seja uma atualização do próprio firmware.

Basicamente, para usar o Boot Seguro, o carregador de OS deve ser assinado com uma chave de confiança do firmware, e você precisa que o carregador de OS verifique se o kernel que ele carrega pode ser confiado.

É possível adicionar Chaves de Troca de Chave (KEK) ao banco de dados de chaves UEFI. Dessa forma, é possível usar outros certificados, desde que sejam assinados com a parte privada da PK.

14.1.1 Implementação no SUSE Linux Enterprise

A Chave de Troca de Chave (KEK) da Microsoft é instalada por padrão.

Nota: GPT (Tabela de Partição GUID) obrigatória

O recurso Boot Seguro requer que a GPT (Tabela de Partição GUID) substitua o particionamento antigo por um MBR (Master Boot Record).

Se o YaST detectar o modo EFI durante a instalação, ele tentará criar uma partição GPT. A UEFI espera encontrar os programas EFI na ESP (Partição de Sistema EFI) formatada por FAT.

O suporte a Boot Seguro UEFI requer basicamente um carregador de boot com assinatura digital que o firmware reconheça como uma chave confiável. Para ser útil aos clientes do SUSE Linux Enterprise, a chave precisa ser, antes de tudo, de confiança do firmware, sem exigir intervenção manual.

Há duas formas de conseguir isso. Uma é trabalhar com os fornecedores do hardware para que eles endossem uma chave do SUSE, que o SUSE usará para assinar o carregador de boot. A outra é utilizar o programa de Certificação de Logotipo do Windows da Microsoft para certificar o carregador de boot e para a Microsoft reconhecer a chave de assinatura do SUSE (isto é, assiná-lo com sua KEK). Até agora, o SUSE assinava o carregador pelo Serviço de Assinatura UEFI (que é a Microsoft, neste caso).

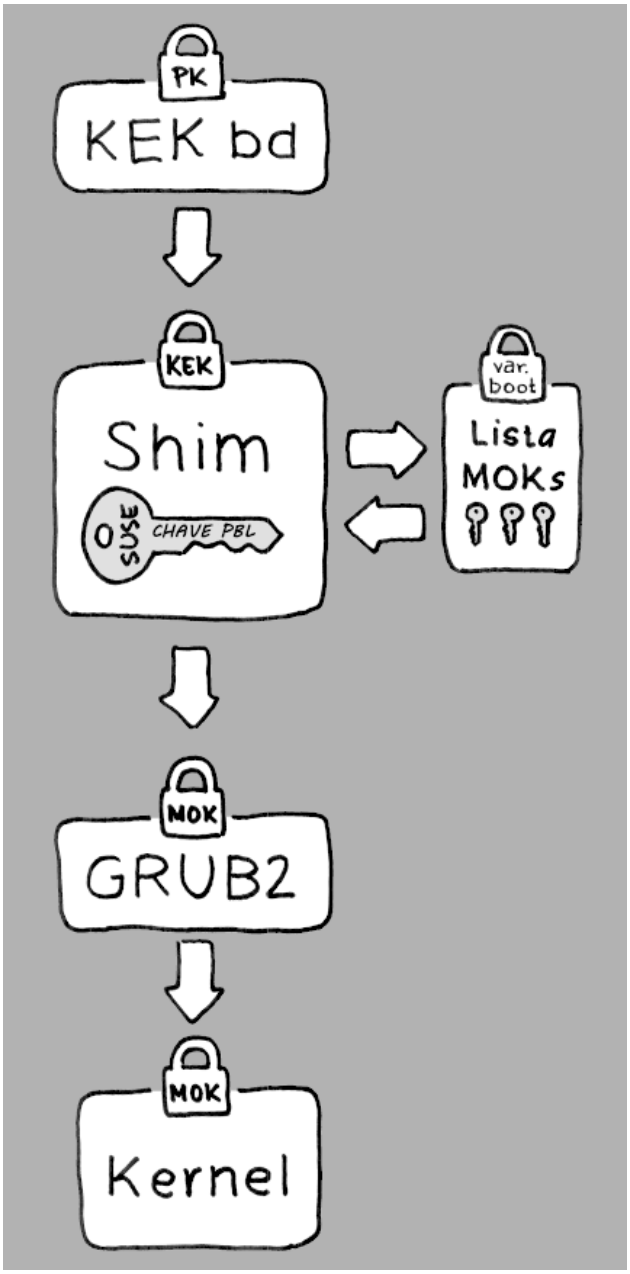


FIGURA 14.1 UEFI: PROCESSO DE BOOT SEGURO

Na camada de implementação, o SUSE usa o carregador `shim`, uma solução inteligente que evita problemas legais e simplifica a etapa de certificação e assinatura consideravelmente. A tarefa do carregador `shim` é carregar um carregador de boot, como eLILO ou GRUB 2 e verificá-lo; e o carregador de boot em troca vai carregar os kernels assinados apenas por uma chave do SUSE. O SUSE oferece esta funcionalidade desde o SLE11 SP3 em instalações novas que tenham o Boot Seguro UEFI habilitado.

Há dois tipos de usuários confiáveis:

- Primeiro, os que detêm as chaves. A Chave de Plataforma (PK) permite quase tudo. A Chave de Troca de Chave (KEK) permite tudo o que pode uma PK, exceto modificar a PK.
- Segundo, qualquer pessoa com acesso físico à máquina. Um usuário com acesso físico pode reinicializar a máquina e configurar a UEFI.

A UEFI oferece dois tipos de variáveis para atender às necessidades desses usuários:

- A primeira são as chamadas “Variáveis Autenticadas”, que podem ser atualizadas tanto do processo de boot (o chamado Ambiente de Serviços de Boot) quanto do OS em execução, mas apenas quando o novo valor da variável é assinado com a mesma chave que assinou o valor antigo da variável. E elas só podem ser anexadas ou modificadas para um valor com número de série maior.
- A segunda são as chamadas “Variáveis Apenas de Serviços de Boot”. Essas variáveis estão acessíveis a qualquer código executado durante o processo de boot. Após o término do processo de boot e antes de iniciar o OS, o carregador de boot deve chamar `ExitBootServices`. Depois disso, essas variáveis não estarão mais acessíveis, e o OS não poderá usá-las.

As várias listas de chaves UEFI são do primeiro tipo, já que permitem atualização online, adição e lista negra de chaves, drivers e impressões digitais do firmware. É o segundo tipo de variável, a “Variável Apenas de Serviços de Boot”, que ajuda a implementar o Boot Seguro de forma segura, pronta para código-fonte aberto e também compatível com GPLv3.

O SUSE começa com o `shim`, um carregador de boot EFI pequeno e simples, que foi originalmente desenvolvido pela Fedora. Ele é assinado por um certificado assinado pela KEK do SUSE e um certificado emitido pela Microsoft, com base nas KEKs disponíveis no banco de dados de chaves UEFI do sistema.

Dessa forma, o `shim` pode ser carregado e executado.

O `shim` continua para verificar se o carregador de boot que deseja carregar é confiável. Em uma situação padrão, o `shim` usa um certificado do SUSE independente incorporado. Além disso, o `shim` permite “inscrever” outras chaves, anulando a chave padrão do SUSE. A seguir, nós as chamamos de “Chaves do Proprietário da Máquina” ou MOKs, para abreviar.

Em seguida, o carregador de boot verifica e inicializa o kernel, e o kernel faz o mesmo com os módulos.

14.1.2 MOK (Chave do Proprietário da Máquina)

Se o usuário (“proprietário da máquina”) deseja substituir algum componente do processo de boot, as Chaves do Proprietário da Máquina (MOKs) deverão ser usadas. A ferramenta `mokutils` ajuda com a assinatura dos componentes e o gerenciamento das MOKs.

O processo de inscrição começa com a reinicialização da máquina e a interrupção do processo de boot (por exemplo, pressionando uma tecla) quando o `shim` é carregado. O `shim` entra no modo de inscrição, permitindo ao usuário substituir a chave padrão do SUSE pelas chaves de um arquivo na partição de boot. Se o usuário quiser, o `shim` calculará um hash desse arquivo e colocará o resultado em uma variável “Apenas de Serviços de Boot”. Dessa forma, o `shim` pode detectar qualquer mudança no arquivo feita fora dos Serviços de Boot e evitar assim uma violação da lista de MOKs aprovadas pelo usuário.

Tudo isso acontece durante a inicialização, apenas o código verificado é executado agora. Portanto, apenas um usuário presente no console pode utilizar o conjunto de chaves do proprietário da máquina. Não é possível que seja um malware ou um invasor com acesso remoto ao OS, pois invasores ou malware só podem mudar o arquivo, mas não o hash armazenado na variável “Apenas de Serviços de Boot”.

O carregador de boot, após ser carregado e verificado pelo `shim`, chamará de novo o `shim` para verificar o kernel, evitando a duplicação do código de verificação. O `shim` usa a mesma lista de MOKs para isso e avisa o carregador de boot se ele pode carregar o kernel.

Dessa forma, você pode instalar seu próprio kernel ou carregador de boot. Só é necessário instalar um novo conjunto de chaves e autorizá-las estando fisicamente presente durante a primeira reinicialização. Como as MOKs são uma lista, e não apenas uma única MOK, é possível fazer com que o `shim` confie nas chaves de vários fornecedores diferentes, permitindo dual-boot e multi-boot pelo carregador de boot.

14.1.3 Inicializando um kernel personalizado

As informações a seguir são baseadas no http://en.opensuse.org/openSUSE:UEFI#Booting_a_custom_kernel.

O Boot Seguro não impede você de usar um kernel autocompilado. Você deve assiná-lo com seu próprio certificado e tornar esse certificado reconhecível para o firmware ou a MOK.

1. Crie uma chave X.509 personalizada e um certificado usados para assinatura:

```
openssl req -new -x509 -newkey rsa:2048 -keyout key.asc \
  -out cert.pem -nodes -days 666 -subj "/CN=$USER/"
```

Para obter mais informações sobre como criar certificados, consulte http://en.opensuse.org/openSUSE:UEFI_Image_File_Sign_Tools#Create_Your_Own_Certificate.

2. Empacote a chave e o certificado como uma estrutura PKCS#12:

```
openssl pkcs12 -export -inkey key.asc -in cert.pem \
  -name kernel_cert -out cert.p12
```

3. Gere um banco de dados NSS para usar com o comando **`pesign`**:

```
certutil -d . -N
```

4. Importe a chave e o certificado incluídos no PKCS#12 para o banco de dados NSS:

```
pk12util -d . -i cert.p12
```

5. “Proteja” o kernel com a nova assinatura usando o comando **`pesign`**:

```
pesign -n . -c kernel_cert -i arch/x86/boot/bzImage \
  -o vmlinuz.signed -s
```

6. Liste as assinaturas na imagem do kernel:

```
pesign -n . -S -i vmlinuz.signed
```

Neste momento, é possível instalar o kernel em `/boot`, como de costume. Como o kernel agora tem uma assinatura personalizada, o certificado usado para a assinatura deve ser importado para o firmware ou a MOK UEFI.

7. Converta o certificado no formato DER para importá-lo para o firmware ou a MOK:

```
openssl x509 -in cert.pem -outform der -out cert.der
```

8. Copie o certificado para o ESP para facilitar o acesso:

```
sudo cp cert.der /boot/efi/
```

9. Use **`mokutil`** para iniciar a lista de MOKs automaticamente.

    a. Importe o certificado para o MOK:

    ```
    mokutil --root-pw --import cert.der
    ```

    A opção `--root-pw` habilita a utilização do usuário `root` diretamente.

    b. Consulte a lista dos certificados preparados para inscrição:

    ```
    mokutil --list-new
    ```

    c. Reinicialize o sistema. O `shim` deve iniciar o MokManager. É necessário digitar a senha de `root` para confirmar a importação do certificado para a lista da MOK.

    d. Verifique se a chave recém-importada foi inscrita:

    ```
    mokutil --list-enrolled
    ```

    a. Se preferir, este é o procedimento para iniciar a MOK manualmente:
    Reinicialize

    b. No menu do GRUB 2, pressione a tecla '`c`'.

    c. Digite:

    ```
    chainloader $efibootdir/MokManager.efi
    boot
    ```

    d. Selecione *Enroll key from disk* (Inscrever chave do disco).

    e. Navegue até o arquivo `cert.der` e pressione `Enter`.

    f. Siga as instruções para inscrever a chave. Normalmente, você pressiona '`0`' e '`y`' para confirmar.
    Se preferir, o menu do firmware pode oferecer maneiras de adicionar uma nova chave ao Banco de Dados de Assinatura.

14.1.4 Recursos e limitações

Ao inicializar no modo Boot Seguro, os seguintes recursos se aplicam:

- Instalação no local do carregador de boot padrão UEFI, um mecanismo para manter ou restaurar a entrada de boot EFI.
- Reinicialização por UEFI.
- O hipervisor do Xen inicializará com UEFI quando não houver nenhum BIOS legado para o qual fazer fallback.
- Suporte a boot PXE IPv6 da UEFI.
- A UEFI oferece suporte ao modo de vídeo. O kernel pode recuperar o modo de vídeo da UEFI para configurar o modo KMS com os mesmos parâmetros.
- A inicialização UEFI de dispositivos USB é suportada.

Ao inicializar no modo Boot Seguro, as seguintes limitações se aplicam:

- Para que o Boot Seguro não seja facilmente desviado, alguns recursos do kernel são desabilitados durante a execução no modo Boot Seguro.
- O carregador de boot, o kernel e os módulos do kernel devem ser assinados.
- Kexec e Kdump estão desabilitados.
- A hibernação (suspensão no disco) é desabilitada.
- O acesso a `/dev/kmem` e `/dev/mem` não é possível, nem mesmo como usuário root.
- O acesso à porta de E/S não é possível, nem mesmo como usuário root. Todos os drivers gráficos X11 devem usar um driver do kernel.
- O acesso a PCI BAR por sysfs não é possível.
- O `custom_method` em ACPI não está disponível.
- Debugfs para o módulo asus-wmi não está disponível.
- O parâmetro `acpi_rsdp` não tem nenhum efeito sobre o kernel.

14.2 Para obter mais informações

- http://www.uefi.org: Home page da UEFI onde você encontra as especificações atuais da UEFI.
- Publicações no blog por Olaf Kirch e Vojtěch Pavlík (o capítulo acima é quase todo baseado nessas publicações):
  - http://www.suse.com/blogs/uefi-secure-boot-plan/
  - http://www.suse.com/blogs/uefi-secure-boot-overview/
  - http://www.suse.com/blogs/uefi-secure-boot-details/
- http://en.opensuse.org/openSUSE:UEFI: UEFI com openSUSE.

15 Recursos especiais do sistema

Este capítulo começa com informações sobre vários pacotes de software, os consoles virtuais e o layout do teclado. Abordamos componentes de software como `bash`, `cron` e `logrotate`, porque eles foram mudados ou aperfeiçoados durante os últimos ciclos de lançamento. Mesmo que eles sejam pequenos ou considerados de menor importância, talvez os usuários desejem mudar o seu comportamento padrão, porque esses componentes muitas vezes estão intimamente ligados ao sistema. O capítulo termina com uma seção sobre configurações específicas de país e idioma (I18N e L10N).

15.1 Informações sobre pacotes de software especiais

Os programas `bash`, `cron`, `logrotate`, `locate`, `ulimit` e `free` são muito importantes para os administradores de sistema e para muitos usuários. As páginas de manual e de informações são duas fontes úteis de informações sobre comandos, mas as duas nem sempre estão disponíveis. O GNU Emacs é um editor de texto popular e muito configurável.

15.1.1 O pacote `bash` e `/etc/profile`

Bash é o shell de sistema padrão. Quando usado com um shell de login, ele lê vários arquivos de inicialização. O Bash os processa na ordem em que são exibidos na lista:

1. `/etc/profile`
2. `~/.profile`

3. `/etc/bash.bashrc`

4. `~/.bashrc`

Faça configurações personalizadas em `~/.profile` ou `~/.bashrc`. Para assegurar o processamento correto desses arquivos, é necessário copiar as configurações básicas de `/etc/skel/.profile` ou `/etc/skel/.bashrc` no diretório pessoal do usuário. É recomendável copiar as configurações de `/etc/skel` após uma atualização. Execute os seguintes comandos de shell para evitar a perda de ajustes pessoais:

```
mv ~/.bashrc ~/.bashrc.old
cp /etc/skel/.bashrc ~/.bashrc
mv ~/.profile ~/.profile.old
cp /etc/skel/.profile ~/.profile
```

Em seguida, copie os ajustes pessoais novamente dos arquivos `*.old`.

15.1.2 O pacote cron

Se você deseja executar comandos de maneira regular e automática em segundo plano em horários predefinidos, cron é a ferramenta a ser usada. O cron é orientado por tabelas de horários especialmente formatadas. Alguns deles vêm com o sistema e os usuários poderão criar suas próprias tabelas, se necessário.

As tabelas cron estão localizadas em `/var/spool/cron/tabs`. `/etc/crontab` atua como uma tabela cron para todo o sistema. Digite o nome de usuário para executar o comando diretamente após a tabela de tempo e antes do comando. No *Exemplo 15.1, "Entrada in /etc/crontab"*, `root` foi inserido. Tabelas específicas de pacote, localizadas em `/etc/cron.d`, possuem o mesmo formato. Consulte a página de manual do **`cron`** (**`man cron`**).

EXEMPLO 15.1 ENTRADA IN /ETC/CRONTAB

```
1-59/5 * * * *   root   test -x /usr/sbin/atrun && /usr/sbin/atrun
```

Você não pode editar `/etc/crontab` chamando o comando **`crontab -e`**. Esse arquivo deve ser carregado diretamente em um editor, modificado e gravado.

Alguns pacotes instalam scripts de shell nos diretórios `/etc/cron.hourly`, `/etc/cron.daily`, `/etc/cron.weekly` e `/etc/cron.monthly`, cuja execução é controlada por `/usr/lib/cron/run-crons`. `/usr/lib/cron/run-crons` é executado a cada 15 minutos da tabela principal (`/etc/crontab`). Isso garante que os processos que tenham sido negligenciados possam ser executados no momento adequado.

Para executar os scripts de manutenção `por hora`, `por dia` ou outros scripts de manutenção periódica em horários personalizados, remova os arquivos de marcação de horário regularmente, utilizando as entradas `/etc/crontab` (consulte o *Exemplo 15.2, "/etc/crontab: remova arquivos de marcação de horário"*, que remove a opção `por hora` antes de cada hora cheia, a opção `por dia` uma vez ao dia às 2:14, etc.).

EXEMPLO 15.2 /ETC/CRONTAB: REMOVA ARQUIVOS DE MARCAÇÃO DE HORÁRIO

```
59 *  * * *     root  rm -f /var/spool/cron/lastrun/cron.hourly
14 2  * * *     root  rm -f /var/spool/cron/lastrun/cron.daily
29 2  * * 6     root  rm -f /var/spool/cron/lastrun/cron.weekly
44 2  1 * *     root  rm -f /var/spool/cron/lastrun/cron.monthly
```

Se preferir, defina `DAILY_TIME` em `/etc/sysconfig/cron` como o horário de início de `cron.daily`. A configuração de `MAX_NOT_RUN` assegura que as tarefas diárias sejam acionadas para execução, mesmo se o usuário não ligou o computador no `DAILY_TIME` especificado por um período mais longo. O valor máximo de `MAX_NOT_RUN` é 14 dias.

Os trabalhos de manutenção diária de sistema são distribuídos a vários scripts por motivos de clareza. Eles estão contidos no pacote `aaa_base`. `/etc/cron.daily` contém, por exemplo, os componentes `suse.de-backup-rpmdb`, `suse.de-clean-tmp` ou `suse.de-cron-local`.

15.1.3 Parando mensagens de status do Cron

Para evitar a inundação de e-mails causada pelas mensagens de status do Cron, o valor padrão de `SEND_MAIL_ON_NO_ERROR` em `/etc/sysconfig/cron` está definido como `"no"` nas novas instalações. Mesmo com essa configuração definida como `"no"`, a saída de dados do Cron ainda será enviada para o endereço `MAILTO`, conforme documentado na página de manual do Cron.

Em caso de atualização, é recomendado definir esses valores de acordo com as suas necessidades.

15.1.4 Arquivos de registro: pacote logrotate

Existem vários serviços de sistema (*daemons*) que, junto com o próprio kernel, gravam regularmente o status do sistema e eventos específicos em arquivos de registro. Dessa maneira, o administrador pode verificar regularmente o status do sistema em um determinado momento, reconhecer erros ou funções defeituosas e solucioná-los com total precisão. Esses arquivos de registro são normalmente armazenados em `/var/log`, como especificado pelo FHS, e crescem diariamente. O pacote `logrotate` ajuda a controlar o crescimento desses arquivos.

Configure o logrotate com o arquivo `/etc/logrotate.conf`. Em particular, a especificação `include` configura principalmente os arquivos adicionais a serem lidos. Programas que produzem arquivos de registro instalam arquivos de configuração individuais em `/etc/logrotate.d`. Por exemplo, esses arquivos vêm com os pacotes `apache2` (`/etc/logrotate.d/apache2`) e `syslog-service` (`/etc/logrotate.d/syslog`).

EXEMPLO 15.3 EXEMPLO PARA /ETC/LOGROTATE.CONF

```
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own lastlog or wtmp - we'll rotate them here
#/var/log/wtmp {
#    monthly
#    create 0664 root utmp
```

```
#    rotate 1
#}


# system-specific logs may be also be configured here.
```

logrotate é controlado pelo cron e é chamado diariamente por `/etc/cron.daily/logrotate`.

Importante: Permissões

A opção `create` lê todas as configurações feitas pelo administrador em `/etc/permissions*`. Certifique-se de que não haja conflitos devido a modificações pessoais.

15.1.5 O comando locate

`locate`, um comando para localização rápida de arquivos, não está incluído no escopo padrão do software instalado. Se desejado, instale o pacote `mlocate`, o sucessor do pacote `findutils-locate`. O processo updatedb é iniciado automaticamente a cada noite ou aproximadamente 15 minutos após a inicialização do sistema.

15.1.6 O comando ulimit

Com o comando **`ulimit`** (*limites do usuário*), é possível definir limites para o uso dos recursos do sistema e fazer com que sejam exibidos. O **`ulimit`** é especialmente útil para limitar a memória disponível para os aplicativos. Com isso, um aplicativo pode ser impedido de absorver recursos em demasia do sistema e deixar o sistema operacional lento ou até travá-lo.

O comando **`ulimit`** pode ser usado com várias opções. Para limitar o uso da memória, use as opções listadas na *Tabela 15.1, "`ulimit`: definindo recursos para o usuário"*.

TABELA 15.1 `ulimit`: DEFININDO RECURSOS PARA O USUÁRIO

`-m`	O tamanho máximo do conjunto residente
`-v`	A quantidade máxima de memória virtual disponível para o shell

`-s`	O tamanho máximo da pilha
`-c`	O tamanho máximo dos arquivos básicos criados
`-a`	Todos os limites atuais são informados

As entradas padrão de todo o sistema estão definidas em `/etc/profile`. Não é recomendado editar esse arquivo diretamente, pois as mudanças serão sobregravadas durante os upgrades do sistema. Para personalizar as configurações de perfil de todo o sistema, use `/etc/profile.local`. Convém efetuar as configurações por usuário em `~USUÁRIO/.bashrc`.

EXEMPLO 15.4 ULIMIT: CONFIGURAÇÕES EM ~/.BASHRC

```
# Limits maximum resident set size (physical memory):
ulimit -m 98304

# Limits of virtual memory:
ulimit -v 98304
```

As alocações de memória devem ser especificadas em KB. Para obter informações mais detalhadas, consulte **`man bash`**.

Importante: Suporte a `ulimit`

Nem todos os shells suportam as diretivas **`ulimit`**. O PAM (por exemplo, `pam_limits`) oferece uma infinidade de possibilidades de ajustes como alternativa ao **`ulimit`**.

15.1.7 O comando free

O comando **`free`** exibe a quantidade total de memória física livre e utilizada e o espaço de troca no sistema, além dos buffers e do cache consumidos pelo kernel. O conceito de *RAM disponível* surgiu antes da época do gerenciamento unificado de memória. O slogan *memória livre é memória ruim* se aplica bem ao Linux. Como resultado, o Linux sempre se esforçou para equilibrar caches externos sem realmente permitir memória livre ou sem uso.

O kernel não tem conhecimento direto de nenhum aplicativo ou dados de usuário. Em vez disso, ele gerencia aplicativos e dados de usuário em um *cache de página*. Se a memória diminuir, partes dele são gravadas na partição de troca ou em arquivos, dos quais podem ser lidas inicialmente com a ajuda do comando **`mmap`** (consulte **`man mmap`**).

O kernel também contém outros caches, como o *cache slab*, onde os caches usados para acesso a rede são armazenados. Isso pode explicar as diferenças entre os contadores em `/proc/meminfo`. A maioria deles (mas não todos) pode ser acessada via `/proc/slabinfo`.

No entanto, se o seu objetivo for descobrir quanta RAM está em uso, encontre essa informação em `/proc/meminfo`.

15.1.8 Páginas de manual e de informações

Para alguns aplicativos GNU (como o tar), as páginas de manuais não são mais mantidas. Para esses comandos, use a opção `--help` para obter uma breve visão geral das páginas de informações, que fornecem instruções mais detalhadas. O info é um sistema de hipertexto do GNU. Leia uma introdução sobre esse sistema digitando **`info`** `info`. As páginas de informações podem ser exibidas com Emacs digitando **`emacs`** `-f info` ou diretamente em um console, com **`info`**. Também é possível usar tkinfo, xinfo ou o sistema de ajuda do para exibir as páginas de informações.

15.1.9 Selecionando páginas de manual usando o comando **`man`**

Para ler a página de manual, digite **`man`** *`página_de_manual`*. Se existir uma página de manual com o mesmo nome em seções diferentes, elas serão listadas com os números da seção correspondentes. Selecione uma para exibir. Se você não digitar um número de seção em alguns segundos, a primeira página de manual será exibida.

Para mudar desse comportamento para o padrão do sistema, defina `MAN_POSIXLY_CORRECT=1` em um arquivo de inicialização de shell, como `~/.bashrc`.

15.1.10 Configurações para GNU Emacs

O GNU Emacs é um complexo ambiente de trabalho. As seções a seguir descrevem os arquivos de configuração processados quando o GNU Emacs é iniciado. Há mais informações em http://www.gnu.org/software/emacs/.

Na inicialização, o Emacs lê vários arquivos que contêm as configurações do usuário, administrador do sistema e distribuidor para personalização ou pré-configuração. O arquivo de inicialização `~/.emacs` é instalado nos diretórios pessoais dos usuários individuais por meio de `/etc/skel`. O `.emacs`, por sua vez, lê o arquivo `/etc/skel/.gnu-emacs`. Para personalizar o programa, copie o arquivo `.gnu-emacs` para o diretório pessoal (com **`cp /etc/skel/.gnu-emacs ~/.gnu-emacs`**) e faça as configurações desejadas nesse diretório.

O `.gnu-emacs` define o arquivo `~/.gnu-emacs-custom` como `arquivo personalizado`. Se os usuários tiverem feito as configurações com as opções `personalizar` no Emacs, as configurações serão gravadas no arquivo `~/.gnu-emacs-custom`.

Com o SUSE Linux Enterprise Desktop, o pacote `emacs` instala o arquivo `site-start.el` no diretório `/usr/share/emacs/site-lisp`. O arquivo `site-start.el` é carregado antes do arquivo de inicialização `~/.emacs`. Entre outras coisas, o arquivo `site-start.el` assegura que os arquivos de configuração especial distribuídos com os pacotes de expansão do Emacs, como o `psgml`, sejam carregados automaticamente. Os arquivos de configuração deste tipo também estão localizados em `/usr/share/emacs/site-lisp`, e sempre começam com o nome `suse-start-`. O administrador do sistema local pode especificar configurações globais do sistema no arquivo `default.el`.

Mais informações sobre esses arquivos estão disponíveis no arquivo de informações do Emacs em *Init File*: `info:/emacs/InitFile`. Informações sobre como desabilitar o carregamento desses arquivos, se necessário, também são fornecidas neste local.

Os componentes do Emacs são divididos em vários pacotes:

- O pacote base `emacs`.
- `emacs-x11` (geralmente instalado): o programa *com* suporte para X11.
- `emacs-nox`: o programa *sem* suporte para X11.
- `emacs-info`: documentação online em formato info.

- `emacs-el`: os arquivos de biblioteca não compilados em Emacs Lisp. Eles não são necessários em tempo de execução.
- Numerosos pacotes complementares podem ser instalados se necessário: `emacs-auctex` (LaTeX), `psgml` (SGML e XML), `gnuserv` (operação cliente e servidor) e outros.

15.2 Consoles virtuais

O Linux é um sistema multiusuário e multitarefa. As vantagens desses recursos podem ser apreciadas mesmo em um sistema de PC independente. No modo de texto, existem seis consoles virtuais disponíveis. Alterne entre eles utilizando as teclas de Alt–F1 até Alt–F6. O sétimo console é reservado para X e o décimo console mostra as mensagens do kernel.

Para alternar para um console de X sem o fechar, use a combinação de teclas de Ctrl–Alt–F1 até Ctrl–Alt–F6. Para voltar para X, pressione Alt–F7.

15.3 Mapeamento de teclado

Para padronizar o mapeamento de teclado de programas, foram feitas mudanças nos seguintes arquivos:

```
/etc/inputrc
/etc/X11/Xmodmap
/etc/skel/.emacs
/etc/skel/.gnu-emacs
/etc/skel/.vimrc
/etc/csh.cshrc
/etc/termcap
/usr/share/terminfo/x/xterm
/usr/share/X11/app-defaults/XTerm
```

```
/usr/share/emacs/VERSION/site-lisp/term/*.el
```

Essas mudanças afetam apenas os aplicativos que usam as entradas **terminfo** ou que têm arquivos de configuração que são modificados diretamente (**vi**, **emacs**, etc.). Os aplicativos que não acompanham o sistema devem ser adaptados a esses padrões.

Em X, a tecla Compose (multitecla) pode ser habilitada conforme explicado em `/etc/X11/Xmodmap`.

Outras configurações são possíveis utilizando-se a Extensão de Teclado X (XKB). Essa extensão também é usada pelos ambientes de área de trabalho do GNOME (gswitchit).

Dica: para obter mais informações

Há informações sobre o XKB disponíveis nos documentos listados em `/usr/share/doc/packages/xkeyboard-config` (parte do pacote `xkeyboard-config`).

15.4 Configurações de idioma e específicas de país

O sistema é, em uma extensão bastante ampla, internacionalizado e pode ser modificado de acordo com as necessidades locais. A internacionalização (*I18N*) permite localizações específicas (*L10N*). As abreviações I18N e L10N são derivadas das primeiras e últimas letras das palavras e, no meio, está o número de letras omitidas.

As configurações são feitas com variáveis `LC_` definidas no arquivo `/etc/sysconfig/language`. Elas referem-se não somente ao *suporte ao idioma nativo*, mas também às categorias *Mensagens* (Idioma), *Conjunto de Caracteres*, *Ordem de Classificação*, *Hora e Data*, *Números* e *Moeda*. Cada uma dessas categorias pode ser definida diretamente com sua própria variável ou indiretamente com uma variável master no arquivo `language` (consulte a página de manual **local**).

`RC_LC_MESSAGES`, `RC_LC_CTYPE`, `RC_LC_COLLATE`, `RC_LC_TIME`, `RC_LC_NUMERIC`, `RC_LC_MONETARY`

Essas variáveis são passadas para o shell sem o prefixo `RC_` e representam as categorias listadas. Os perfis shell de referência estão listados abaixo. A configuração atual pode ser exibida com o comando **locale**.

`RC_LC_ALL`

Essa variável, se definida, sobregrava os valores das variáveis já mencionadas.

`RC_LANG`

Se nenhuma das variáveis anteriores for definida, esse é o fallback. Por padrão, apenas `RC_LANG` está definida. Isso facilita o processo para que os usuários informem seus próprios valores.

`ROOT_USES_LANG`

Uma variável `yes` ou `no`. Se for definida como `no`, `root` sempre funcionará no ambiente POSIX.

As variáveis podem ser definidas com o editor sysconfig do YaST. O valor dessa variável contém o código do idioma, código do país, codificação e modificador. Os componentes individuais são conectados por caracteres especiais:

```
LANG=<language>[[_<COUNTRY>].<Encoding>[@<Modifier>]]
```

15.4.1 Alguns exemplos

Você deve sempre definir os códigos do idioma e do país juntos. As configurações do idioma seguem o padrão ISO 639 disponível em http://www.evertype.com/standards/iso639/iso639-en.html e http://www.loc.gov/standards/iso639-2/. Os códigos de país estão listados em ISO 3166, consulte http://en.wikipedia.org/wiki/ISO_3166.

Só faz sentido definir valores para os quais os arquivos de descrição utilizáveis podem ser encontrados em `/usr/lib/locale`. Arquivos de descrição adicionais podem ser criados de arquivos em `/usr/share/i18n` utilizando o comando **`localedef`**. Os arquivos de descrição fazem parte do pacote `glibc-i18ndata.` Um arquivo de descrição para `en_US.UTF-8` (para inglês e Estados Unidos) pode ser criado com:

```
localedef -i en_US -f UTF-8 en_US.UTF-8
```

`LANG=en_US.UTF-8`

Essa é a configuração padrão se Inglês americano for selecionado durante a instalação. Se você tiver selecionado outro idioma, ele será habilitado, mas ainda terá o UTF-8 como codificação de caractere.

`LANG=en_US.ISO-8859-1`

Define o idioma como inglês, o país como Estados Unidos e o conjunto de caracteres como `ISO-8859-1`. Essa definição de caractere não suporta o sinal de Euro, mas às vezes pode ser útil para programas que não foram atualizados para suportar `UTF-8`. A string que define o conjunto de caracteres (`ISO-8859-1` nesse caso) é então avaliada por programas como o Emacs.

`LANG=en_IE@euro`

O exemplo acima inclui explicitamente o sinal de Euro em uma configuração de idioma. Essa configuração está obsoleta agora, pois o UTF-8 também abrange o símbolo do Euro. Será útil apenas se um aplicativo suportar ISO-8859-15 e não UTF-8.

As mudanças em `/etc/sysconfig/language` são ativadas pela seguinte cadeia de processo:

- Para Bash: `/etc/profile` lê `/etc/profile.d/lang.sh` que, por sua vez, analisa `/etc/sysconfig/language`.
- Para tcsh: No login, `/etc/csh.login` lê `/etc/profile.d/lang.csh` que, por sua vez, analisa `/etc/sysconfig/language`.

Isso garante que toda mudança em `/etc/sysconfig/language` fique disponível no próximo login para o respectivo shell, sem ter que ativá-la manualmente.

Os usuários anular os padrões do sistema editando o seu `~/.bashrc` da maneira adequada. Por exemplo, se você não deseja usar `en_US` em todo o sistema para mensagens de programa, em vez disso, inclua `LC_MESSAGES=es_ES` para exibir as mensagens em espanhol.

15.4.2 Configurações locais em `~/.i18n`

Se não estiver satisfeito com os padrões do sistema local, mude as configurações em `~/.i18n` de acordo com a sintaxe de script Bash. As entradas em `~/.i18n` substituem os padrões do sistema de `/etc/sysconfig/language`. Use os mesmos nomes de variáveis, mas sem os prefixos de namespace `RC_`. Por exemplo, use `LANG` em vez de `RC_LANG`:

```
LANG=cs_CZ.UTF-8
```

```
LC_COLLATE=C
```

15.4.3 Configurações de suporte de idioma

Arquivos na categoria *Mensagens* são, via de regra, armazenados somente no diretório do idioma correspondente (como `en`) para ter um fallback. Se você definir `LANG` para `en_US` e o arquivo de mensagem em `/usr/share/locale/en_US/LC_MESSAGES` não existir, ele voltará para `/usr/share/locale/en/LC_MESSAGES`.

Uma cadeia de fallback também pode ser definida, por exemplo, para bretão para francês ou galego para espanhol para português:

`LANGUAGE="br_FR:fr_FR"`

`LANGUAGE="gl_ES:es_ES:pt_PT"`

Se desejar, use as variantes norueguesas Nynorsk e Bokmål (com fallback adicional para `no`):

`LANG="nn_NO"`

`LANGUAGE="nn_NO:nb_NO:no"`

ou

`LANG="nb_NO"`

`LANGUAGE="nb_NO:nn_NO:no"`

Observe que em norueguês, `LC_TIME` também é tratado de maneira diferente.

Um problema que pode surgir é um separador usado para delimitar grupos de dígitos não ser reconhecido corretamente. Isso acontece se `LANG` for definido para um código de idioma com somente duas letras, como `de`, mas o arquivo de definição que o glibc utiliza estiver localizado em `/usr/share/lib/de_DE/LC_NUMERIC`. Por isso, `LC_NUMERIC` deve ser definido como `de_DE` para tornar a definição de separador visível para o sistema.

15.4.4 Para obter mais informações

- *The GNU C Library Reference Manual*, Capítulo “Locales and Internationalization”. Ele está incluído em `glibc-info`. O pacote está disponível no SDK do SUSE Linux Enterprise. O SDK é um produto complementar do SUSE Linux Enterprise e está disponível para download pelo site http://download.suse.com/. Pesquise por `SUSE Linux Enterprise Software Development Kit`.
- Markus Kuhn, *UTF-8 and Unicode FAQ for Unix/Linux*, atualmente em http://www.cl.cam.ac.uk/~mgk25/unicode.html.
- *Unicode-HOWTO* por Bruno Haible, disponível em http://tldp.org/HOWTO/Unicode-HOWTO-1.html.

16 Operação da impressora

O SUSE® Linux Enterprise Desktop suporta a impressão com muitos tipos de impressoras, incluindo impressoras de rede remotas. É possível configurar as impressoras manualmente ou com o YaST. Para obter instruções de configuração, consulte a *Book "Deployment Guide" 5 "Setting Up Hardware Components with YaST" 5.3 "Setting Up a Printer"*. Os utilitários gráficos e de linha de comando estão disponíveis para iniciar e gerenciar serviços de impressão. Se a sua impressora não funcionar como se esperava, consulte a *Seção 16.8, "Solução de problemas"*.

CUPS (Common Unix Printing System) é o sistema de impressão padrão no SUSE Linux Enterprise Desktop.

As impressoras podem ser distinguidas pela interface, como USB ou rede, e pela linguagem de impressão. Ao comprar uma impressora, verifique se a sua interface é suportada (USB, Ethernet ou Wi-Fi) e se a sua linguagem é adequada. As impressoras podem ser categorizadas com base em três classes de linguagem:

Impressoras PostScript

PostScript é a linguagem de impressora na qual a maior parte dos serviços de impressão em Linux e Unix são gerados e processados pelo sistema de impressão interno. Se documentos PostScript puderem ser diretamente processados pela impressora e não precisarem ser convertidos em estágios adicionais do sistema de impressão, o número de origens de erro potenciais será reduzido.

Atualmente, o PostScript vem sendo substituído pelo PDF como o formato padrão dos serviços de impressão. Já existem impressoras PostScript + PDF que imprimem diretamente em PDF (e também em PostScript). Para as impressoras PostScript tradicionais, é necessário converter de PDF em PostScript no workflow de impressão.

Impressora padrão (linguagens como PCL e ESC/P)

No caso de linguagens conhecidas, o sistema pode converter tarefas de impressão PostScript na respectiva linguagem de impressão com a ajuda do Ghostscript. Esta fase do processamento é chamada de interpretação. As linguagens mais conhecidas são PCL (mais usada pelas impressoras HP e seus clones) e ESC/P (utilizada nas impressoras Epson). Geralmente, essas linguagens são suportadas no Linux e produzem um resultado de impressão adequado. O Linux pode não conseguir realizar algumas funções especiais da impressora. Com exceção da HP e da Epson, não há fabricantes de impressoras que desenvolvem e disponibilizam drivers de Linux a distribuidores Linux sob uma licença de código-fonte aberto.

Impressoras proprietárias (também denominadas impressoras GDI)

Essas impressoras não suportam nenhuma das linguagens de impressora comuns. Elas usam suas próprias linguagens de impressora não documentadas, que ficam sujeitas a mudanças quando é lançada uma edição nova de um modelo. Geralmente, apenas os drivers do Windows estão disponíveis para essas impressoras. Consulte a *Seção 16.8.1, "Impressoras sem suporte de linguagem de impressora padrão"* para obter mais informações.

Antes de comprar uma nova impressora, consulte as seguintes fontes para verificar a abrangência do suporte ao equipamento pretendido:

http://www.linuxfoundation.org/OpenPrinting/

A home page OpenPrinting com o banco de dados de impressão. O banco de dados mostra o status mais recente de suporte do Linux. No entanto, a distribuição do Linux só pode integrar os drivers disponíveis no momento da produção. Da mesma forma, uma impressora atualmente classificada como "perfeitamente suportada" talvez não apresentasse esse status quando a versão mais recente do SUSE Linux Enterprise Desktop foi lançada. Assim, os bancos de dados não indicarão necessariamente o status correto, mas apenas uma informação aproximada.

http://pages.cs.wisc.edu/~ghost/

Página do Ghostscript na Web.

`/usr/share/doc/packages/ghostscript/catalog.devices`

Lista de drivers Ghostscript incorporados.

16.1 O workflow do CUPS

O usuário cria um serviço de impressão. O serviço de impressão consiste nos dados a serem impressos e nas informações para o spooler, como nome da impressora ou nome da fila de impressão e, opcionalmente, nas informações para o filtro, como opções específicas da impressora.

Existe pelo menos uma fila de impressão dedicada para cada impressora. O spooler mantém o serviço de impressão em fila até que a impressora desejada esteja pronta para receber dados. Uma vez pronta, o spooler envia os dados pelo filtro, tendo a impressora como back end.

O filtro converte os dados gerados pelo aplicativo que está imprimindo (geralmente PostScript ou PDF, mas também ASCII, JPEG e outros) em dados específicos da impressora (PostScript, PCL, ESC/P etc.). Os recursos da impressora são descritos nos arquivos PPD. O arquivo PPD contém opções da impressora com os parâmetros necessários para habilitá-los. O sistema de filtros verifica se as opções selecionadas pelo usuário foram habilitadas.

Se você usa uma impressora PostScript, o sistema de filtros converte os dados em PostScript específico da impressora. Isso não exige um driver de impressora. Se você usa uma impressora não PostScript, o sistema de filtros converte os dados em dados específicos da impressora. Isso exige um driver adequado à sua impressora. O back end recebe do filtro os dados específicos da impressora e os repassa a ela.

16.2 Métodos e protocolos de conexão de impressoras

Existem várias possibilidades para conectar uma impressora ao sistema. A configuração do sistema de impressão CUPS não faz distinção entre uma impressora local e uma impressora conectada ao sistema pela rede. Para obter mais informações sobre a conexão de impressoras, leia o artigo *CUPS in a Nutshell* (CUPS numa Casca de Noz) em http://en.opensuse.org/SDB:CUPS_in_a_Nutshell.

Atenção: mudando as conexões de cabo em um sistema em execução

Ao conectar a impressora à máquina, não esqueça de que apenas dispositivos USB podem ser conectados ou desconectados durante a operação. Para evitar danos ao sistema ou à impressora, encerre o sistema antes de mudar qualquer conexão que não seja USB.

16.3 Instalando o software

PPD (descrição de impressora PostScript) é a linguagem de computador que descreve as propriedades, como resolução, e as opções, como disponibilidade de uma unidade duplex. Essas descrições são necessárias para o uso de várias opções de impressora no CUPS. Sem um arquivo PPD, os dados de impressão seriam encaminhados à impressora em estado “bruto”, o que normalmente não é desejado.

Para configurar uma impressora PostScript, a melhor opção é obter um arquivo PPD adequado. Muitos arquivos PPD estão disponíveis nos pacotes `manufacturer-PPDs` e `OpenPrintingPPDs-postscript`. Consulte a *Seção 16.7.3, "Arquivos PPD em pacotes diferentes"* e a *Seção 16.8.2, "Nenhum arquivo PPD adequado disponível para impressora PostScript"*.

É possível armazenar novos arquivos PPD no diretório `/usr/share/cups/model/` ou adicioná-los ao sistema de impressão com o YaST, conforme descrito na *Book "Deployment Guide" 5 "Setting Up Hardware Components with YaST"5.3.1.1 "Adding Drivers with YaST"*. Na sequência, é possível selecionar o arquivo PPD durante a configuração da impressora.

Observe se o fabricante da impressora requer que você instale pacotes inteiros de software. Primeiro, esse tipo de instalação pode resultar na perda do suporte oferecido pelo SUSE Linux Enterprise Desktop e, segundo, os comandos de impressão podem funcionar de forma diferente e o sistema pode não conseguir mais trabalhar com dispositivos de outros fabricantes. Por isso, não recomendamos instalar o software do fabricante.

16.4 Impressoras de rede

Uma impressora de rede pode suportar vários protocolos, alguns deles até simultaneamente. Embora a maioria dos protocolos suportados seja padronizada, alguns fabricantes modificam o padrão. Os fabricantes então fornecem drivers apenas para alguns sistemas operacionais. Infelizmente, raros são os drivers para Linux. Na situação atual, não é possível agir como se todos os protocolos funcionassem perfeitamente no Linux. Portanto, talvez seja necessário testar várias opções para chegar a uma configuração funcional.

O CUPS suporta os protocolos `socket`, `LPD`, `IPP` e `smb`.

socket

Socket refere-se a uma conexão em que os dados de impressão simples são enviados diretamente a um soquete TCP. Alguns dos números de portas de soquete normalmente usados são `9100` ou `35`. A sintaxe do URI (uniform resource identifier) do dispositivo é: socket://*`IP.da.impressora`*:*`porta`*, por exemplo: `socket://192.168.2.202:9100/`.

LPD (Line Printer Daemon)

O protocolo LPD está descrito no RFC 1179. Nesse protocolo, alguns dados relacionados ao serviço, como o ID da fila de impressão, são enviados antes dos dados da impressão propriamente ditos. Portanto, a fila de impressão deve ser especificada no momento da configuração do protocolo LPD. As implementações de fabricantes de impressoras

diferentes são flexíveis o suficiente para aceitar qualquer nome como a fila de impressão. Se necessário, o manual da impressora indicará o nome a ser usado. Geralmente se usa LPT, LPT1, LP1 ou nomes semelhantes. O número de porta para o serviço LPD é `515`. Um exemplo de URI de dispositivo é `lpd://192.168.2.202/LPT1`.

IPP (Internet Printing Protocol)

IPP é um protocolo relativamente novo (1999) baseado no protocolo HTTP. Com o IPP, mais dados referentes à tarefa são transmitidos. O CUPS usa o IPP em transmissões internas de dados. É necessário indicar o nome da fila de impressão para que o IPP seja configurado corretamente. A porta padrão do IPP é `631`. Exemplos de URIs de dispositivo: `ipp://192.168.2.202/ps` e `ipp://192.168.2.202/impressoras/ps`.

SMB (compartilhamento Windows)

O CUPS também suporta a impressão em impressoras conectadas a compartilhamentos Windows. O protocolo usado para essa finalidade é o SMB. O SMB usa os números de porta `137`, `138` e `139`. Exemplos de URIs de dispositivo: `smb://usuário:senha@grupo_de_trabalho/smb.exemplo.com/printer`, `smb://usuário:senha@smb.exemplo.com/impressora` e `smb://smb.exemplo.com/impressora`.

O protocolo suportado pela impressora deve ser determinado antes da configuração. Se o fabricante não fornecer as informações necessárias, o comando **`nmap`** (que vem com o pacote `nmap`) pode ser usado para verificar o protocolo. O **`nmap`** verifica se há portas abertas em um host. Por exemplo:

```
nmap -p 35,137-139,515,631,9100-10000 printerIP
```

16.5 Configurando o CUPS com ferramentas da linha de comando

É possível configurar o CUPS com ferramentas de linha de comando, como **`lpinfo`**, **`lpadmin`** e **`lpoptions`**. Você precisa de um URI de dispositivo composto por um back end, como USB, e parâmetros. Para determinar os URIs de dispositivo válidos no sistema, use o comando **`lpinfo -v | grep ":/"`**:

```
# lpinfo -v | grep ":/"
```

```
direct usb://ACME/FunPrinter%20XL
network socket://192.168.2.253
```

Com o **lpadmin**, o administrador do servidor CUPS pode adicionar, remover ou gerenciar filas de impressão. Para adicionar uma fila de impressão, use a seguinte sintaxe:

```
lpadmin -p queue -v device-URI -P PPD-file -E
```

Em seguida, o dispositivo (`-v`) fica disponível como *fila* (`-p`), usando o arquivo PPD especificado (`-P`). Isso significa que você precisa saber qual é o arquivo PPD e o URI de dispositivo para configurar a impressora manualmente.

Não use `-E` como primeira opção. Em todos os comandos CUPS, `-E` como primeiro argumento define o uso de uma conexão criptografada. Para habilitar a impressora, `-E` deve ser usado como mostrado no seguinte exemplo:

```
lpadmin -p ps -v usb://ACME/FunPrinter%20XL -P \
/usr/share/cups/model/Postscript.ppd.gz -E
```

O seguinte exemplo configura uma impressora de rede:

```
lpadmin -p ps -v socket://192.168.2.202:9100/ -P \
/usr/share/cups/model/Postscript-level1.ppd.gz -E
```

Para conhecer mais opções de **lpadmin**, consulte a página de manual de `lpadmin(8)`.

Durante a configuração da impressora, algumas opções são definidas como padrão. Essas opções podem ser modificadas para cada serviço de impressão (dependendo da ferramenta de impressão utilizada). Também é possível modificar essas opções padrão com o YaST. Usando ferramentas de linha de comando, defina opções padrão da seguinte forma:

1. Primeiro, liste todas as opções:

   ```
   lpoptions -p queue -l
   ```

   Exemplo:

   ```
   Resolution/Output Resolution: 150dpi *300dpi 600dpi
   ```

   A opção padrão ativada é identificada por um asterisco na frente (`*`).

2. Mude a opção com **lpadmin**:

```
lpadmin -p queue -o Resolution=600dpi
```

3. Verifique a nova configuração:

```
lpoptions -p queue -l

Resolution/Output Resolution: 150dpi 300dpi *600dpi
```

Quando um usuário comum executa **lpoptions**, as configurações são gravadas em `~/.cups/lpoptions`. Porém, as configurações de `root` são gravadas em `/etc/cups/lpoptions`.

16.6 Imprimindo pela linha de comando

Para imprimir pela linha de comando, digite **lp-d** *nome da fila nome do arquivo*, substituindo *nome da fila* e *nome do arquivo* pelos nomes correspondentes.

Alguns aplicativos dependem do comando **lp** para imprimir. Nesse caso, digite o comando correto na caixa de diálogo do aplicativo, geralmente sem especificar *nome do arquivo*, por exemplo **lp -d***nome da fila*.

16.7 Recursos especiais no SUSE Linux Enterprise Desktop

Vários recursos do CUPS foram adaptados para o SUSE Linux Enterprise Desktop. Algumas das mudanças mais importantes são abordadas aqui.

16.7.1 CUPS e firewall

Após realizar a instalação padrão do SUSE Linux Enterprise Desktop, o SuSEFirewall2 será ativado e as interfaces de rede serão configuradas para ficarem na `Zona Externa`, que bloqueia o tráfego de entrada. Há mais informações sobre a configuração do SuSEFirewall2 disponíveis na *Book "*Security Guide*" 15 "Masquerading and Firewalls"15.4 "SuSEFirewall2"* e em http://en.opensuse.org/SDB:CUPS_and_SANE_Firewall_settings.

16.7.1.1 Cliente CUPS

Normalmente, um cliente CUPS é executado em uma estação de trabalho comum, localizada em um ambiente de rede confiável protegido por firewall. Neste caso, é recomendável configurar a interface de rede para ficar na `Zona Interna`, de modo que a estação de trabalho possa ser alcançada de dentro da rede.

16.7.1.2 Servidor CUPS

Se o servidor CUPS fizer parte de um ambiente de rede confiável, protegido por um firewall, a interface de rede deverá ser configurada para ficar na `Zona Interna` do firewall. Não é recomendado configurar um servidor CUPS em um ambiente de rede não confiável, a menos que você tenha o cuidado de mantê-lo protegido por regras especiais de firewall e opções seguras na configuração do CUPS.

16.7.2 Procurando impressoras de rede

Os servidores CUPS anunciam regularmente as informações sobre disponibilidade e status das impressoras compartilhadas na rede. Os clientes podem acessar essas informações para exibir uma lista de impressoras disponíveis nas caixas de diálogo de impressão, por exemplo. Isso se chama “procurar”.

Os servidores CUPS anunciam suas filas de impressão pela rede usando o protocolo de pesquisa tradicional do CUPS ou o Bonjour/DND-SD. Para procurar filas de impressão de rede, o serviço `cups-browsed` deve ser executado em todos os clientes que imprimem por meio de servidores CUPS. O `cups-browsed` não é iniciado por padrão. Para iniciá-lo na sessão ativa, use **`sudo systemctl start cups-browsed.service`**. Para assegurar que ele seja iniciado automaticamente após a inicialização, habilite-o com **`sudo systemctl enable cups-browsed.service`** em todos os clientes.

Caso a pesquisa não funcione depois de iniciar `cups-browsed`, o(s) servidor(es) CUPS provavelmente anunciará(ão) as filas da impressora de rede por Bonjour/DND-SD. Neste caso, é necessário instalar adicionalmente o pacote `avahi` e iniciar o serviço associado ao **`sudo systemctl start avahi-daemon.service`** em todos os clientes.

16.7.3 Arquivos PPD em pacotes diferentes

A configuração de impressora do YaST define as filas do CUPS usando os arquivos PPD instalados em `/usr/share/cups/model`. Para localizar os arquivos PPD adequados ao modelo da impressora, o YaST compara o fornecedor e o modelo determinados durante a detecção de hardware com os fornecedores e modelos em todos os arquivos PPD. Para isso, a configuração de impressora do YaST gera um banco de dados com as informações de fabricante e modelo extraídas dos arquivos PPD.

A configuração com apenas arquivos PPD e nenhuma outra fonte de informação tem a vantagem de permitir a livre modificação de arquivos PPD em `/usr/share/cups/model/`. Por exemplo, se você possui impressoras PostScript, será possível copiar os arquivos PPD diretamente para `/usr/share/cups/model` (se ainda não existirem nos pacotes `manufacturer-PPDs` ou `OpenPrintingPPDs-postscript`) para atingir a configuração ideal para as suas impressoras.

Os arquivos PPD adicionais são fornecidos pelos seguintes pacotes:

- gutenprint: o driver Gutenprint e seus PPDs correspondentes
- splix: o driver SpliX e seus PPDs correspondentes
- OpenPrintingPPDs-ghostscript: os PPDs para os drivers Ghostscript incorporados
- OpenPrintingPPDs-hpijs: os PPDs para o driver HPIJS para impressoras não HP

16.8 Solução de problemas

As seções a seguir abordam alguns dos problemas mais encontrados em relação a hardware e software de impressora, bem como formas de solucionar ou superar esses problemas. Os tópicos abordados incluem impressoras GDI, arquivos PPD e configuração de porta. Problemas comuns de impressoras de rede, impressões com defeito e gerenciamento de filas também são tratados.

16.8.1 Impressoras sem suporte de linguagem de impressora padrão

Essas impressoras não suportam nenhuma linguagem de impressora comum, podendo apenas ser tratadas com sequências especiais de controle proprietário. Portanto, elas só funcionam com as versões de sistema operacional para as quais o fabricante fornece driver. GDI é uma interface de

programação desenvolvida pela Microsoft* para dispositivos gráficos. Geralmente o fabricante fornece drivers apenas para Windows e, com o driver do Windows usa a interface GDI, essas impressoras também são chamadas de *impressoras GDI*. O verdadeiro problema não é a interface de programação, mas o fato de que tais impressoras só podem ser tratadas com a linguagem de impressora proprietária do respectivo modelo de impressora.

Algumas impressoras GDI podem ser ajustadas para funcionar no modo GDI ou em uma das linguagens de impressora padrão. Consulte o manual da impressora para saber se isso é possível. Alguns modelos exigem software especial do Windows para fazer o ajuste (observe que o driver de impressora do Windows pode sempre retornar a impressora para o modo GDI quando se imprime do Windows). Para outras impressoras GDI, existem módulos de extensão disponíveis para uma linguagem de impressora padrão.

Alguns fabricantes oferecem drivers proprietários para suas impressoras A desvantagem dos drivers de impressora proprietários é que não há garantia de que vão funcionar com o sistema de impressão instalado ou de que sejam adequados para as diferentes plataformas de hardware. Em contraste, impressoras que suportam uma linguagem de impressora padrão não dependem de uma versão do sistema de impressão especial ou de plataforma de hardware especial.

Em vez de perder tempo tentando fazer funcionar um driver de Linux proprietário, a compra de uma impressora que suporte a linguagem padrão de impressora (preferencialmente PostScript) pode ter melhor custo-benefício. Isso soluciona o problema do driver de uma vez por todas, eliminando a necessidade de instalar e configurar software de driver especial e obter atualizações de driver que talvez fossem necessárias por causa de novos avanços no sistema de impressão.

16.8.2 Nenhum arquivo PPD adequado disponível para impressora PostScript

Se o pacote `manufacturer-PPDs` ou `OpenPrintingPPDs-postscript` não incluir o arquivo PPD adequado para uma impressora PostScript, será possível utilizar o arquivo PPD do CD do driver do fabricante da impressora ou fazer download de um arquivo PPD adequado da página do fabricante da impressora na Web.

Se o arquivo PPD for fornecido como arquivo compactado (.zip) ou arquivo compactado de autoextração (`.exe`), faça a descompactação com **`unzip`**. Primeiro, reveja os termos de licença do arquivo PPD. Em seguida, use o utilitário **`cupstestppd`** para verificar se o arquivo PPD atende à “Especificação de Formato de Arquivo PPD (PostScript Printer Description — Descrição

de Impressora PostScript) da Adobe, versão 4.3". Se o utilitário retornar "FAIL", significa que os erros nos arquivos PPD são graves e provavelmente causam os principais problemas. Os problemas reportados pelo **cupstestppd** devem ser eliminados. Se necessário, peça o arquivo PPD adequado ao fabricante da impressora.

16.8.3 Conexões da impressora de rede

Identificação de problemas de rede

Conecte a impressora diretamente ao computador. Para fins de teste, configure-a como impressora local. Se isso funcionar, o problema está na rede.

Verificando a rede TCP/IP

A rede TCP/IP e a resolução de nomes devem ser funcionais.

Verificando um `lpd` remoto

Use o comando a seguir para testar o estabelecimento de uma conexão TCP com **lpd** (porta `515`) no *`host`*.

```
netcat -z host 515 && echo ok || echo failed
```

Se a conexão com **lpd** não for estabelecida, o **lpd** pode não estar ativo ou pode haver problemas básicos de rede.

Como usuário `root`, use o seguinte comando para consultar um relatório de status (possivelmente muito longo) sobre a *`fila`* no *`host`* remoto, considerando que o respectivo **lpd** esteja ativo e o host aceite consultas:

```
echo -e "\004queue" \
| netcat -w 2 -p 722 host 515
```

Se o **lpd** não responder, ele pode não estar ativo ou pode haver problemas básicos de rede. Se o **lpd** responder, a resposta deverá mostrar por que não é possível imprimir na `fila` do `host`. Se você receber uma resposta como esta, mostrada no *Exemplo 16.1, "Mensagem de erro do* **lpd***"*, significa que o problema está sendo causado pelo **lpd** remoto.

EXEMPLO 16.1 MENSAGEM DE ERRO DO `lpd`

```
lpd: your host does not have line printer access
lpd: queue does not exist
```

```
printer: spooling disabled
printer: printing disabled
```

Verificando um `cupsd` remoto

Um servidor de rede CUPS pode transmitir suas filas por padrão a cada 30 segundos na porta UDP `631`. Conforme apresentado, os seguintes comandos podem ser usados para testar se existe um servidor de rede CUPS de broadcasting na rede. Não deixe de parar seu daemon CUPS local antes de executar o comando.

```
netcat -u -l -p 631 & PID=$! ; sleep 40 ; kill $PID
```

Se existir um servidor de rede CUPS de transmissão, a saída aparecerá conforme mostrado no *Exemplo 16.2, "Transmissão do servidor de rede CUPS"*.

EXEMPLO 16.2 TRANSMISSÃO DO SERVIDOR DE REDE CUPS

```
ipp://192.168.2.202:631/printers/queue
```

Use o comando a seguir para testar o estabelecimento de uma conexão TCP com **`cupsd`** (porta `631`) no *`host`*.

```
netcat -z host 631 && echo ok || echo failed
```

Se não for possível estabelecer a conexão com **`cupsd`**, pode ser que o **`cupsd`** não esteja ativo ou existam problemas básicos de rede. **`lpstat -h`** *`host`* **`-l -t`** retorna um relatório de status (possivelmente muito longo) de todas as filas do *`host`*, contanto que o respectivo **`cupsd`** esteja ativo e o host aceite consultas.

O próximo comando pode ser usado para testar se a *`fila`* do *`host`* aceita um serviço de impressão que consiste em um único caractere de retorno de carro. Nada será impresso. Possivelmente, será ejetada uma página em branco.

```
echo -en "\r" \
| lp -d queue -h host
```

Solução de problemas da impressora de rede ou da caixa do servidor de impressão

Algumas vezes, spoolers executados na caixa do servidor de impressão causam problemas quando precisam lidar com vários serviços de impressão. Como isso é causado pelo spooler na caixa do servidor de impressão, não há como resolver essa questão. Como solução

alternativa, desvie o spooler na caixa do servidor de impressão endereçando a impressora conectada à caixa diretamente com o soquete TCP. Consulte a *Seção 16.4, "Impressoras de rede"*.

Dessa forma, a caixa do servidor de impressão é reduzida a um conversor entre as várias formas de transferência de dados (conexão de rede TCP/IP e impressora local). Para usar esse método, você precisa conhecer a porta TCP da caixa do servidor de impressão. Se a impressora estiver conectada à caixa do servidor de impressão e ligada, a porta TCP poderá ser determinada normalmente com o utilitário **`nmap`** do pacote `nmap`, algum tempo depois que a caixa for ativada. Por exemplo, **`nmap`** *`endereço IP`* pode gerar o seguinte resultado para uma caixa do servidor de impressão:

```
Port       State       Service
23/tcp     open        telnet
80/tcp     open        http
515/tcp    open        printer
631/tcp    open        cups
9100/tcp   open        jetdirect
```

Essa saída indica que a impressora conectada à caixa do servidor de impressão pode ser endereçada via soquete TCP na porta `9100`. Por padrão, **`nmap`** verifica somente algumas portas mais conhecidas listadas em `/usr/share/nmap/nmap-services`. Para verificar todas as portas possíveis, use o comando **`nmap -p`** *`porta_de_origem-porta_de_destino endereço_IP`*. O processo pode levar algum tempo. Para obter mais informações, consulte a página de manual de **`nmap`**.

Digite um comando como

```
echo -en "\rHello\r\f" | netcat -w 1 IP-address port
cat file | netcat -w 1 IP-address port
```

para enviar strings de caracteres ou arquivos diretamente à respectiva porta para testar se a impressora pode ser endereçada dessa porta.

16.8.4 Defeitos na impressão sem mensagem de erro

Para o sistema de impressão, o serviço de impressão é concluído quando o back end do CUPS conclui a transferência de dados ao destinatário (impressora). Se houver falha no processamento posterior no destinatário (por exemplo, se a impressora não imprimir seus próprios dados específicos), o sistema de impressão não notará. Se a impressora não imprimir seus próprios dados específicos, selecione um arquivo PPD mais adequado à impressora.

16.8.5 Filas desabilitadas

Se a transferência de dados para o destinatário falhar completamente após várias tentativas, o back end do CUPS, como `USB` ou `socket`, reportará um erro ao sistema de impressão (ao **`cupsd`**). O back end determina quantas tentativas malsucedidas são necessárias para que a transferência de dados seja considerada impossível. Visto que as tentativas posteriores serão inúteis, o **`cupsd`** desabilita a impressão da fila correspondente. Após resolver a causa do problema, o administrador do sistema deve reabilitar a impressão com o comando **`cupsenable`**.

16.8.6 Navegação do CUPS: apagando serviços de impressão

Se um servidor de rede CUPS transmitir suas filas aos hosts de clientes via navegação e um **`cupsd`** local adequado estiver ativo nos hosts de clientes, o **`cupsd`** de cliente aceitará serviços de impressão de aplicativos e os encaminhará ao **`cupsd`** no servidor. Quando **`cupsd`** no servidor aceitar um serviço de impressão, ele receberá um novo número de serviço. Portanto, o número da tarefa no host cliente é diferente do número da tarefa no servidor. Como geralmente um serviço de impressão é encaminhado de imediato, não é possível apagá-lo com o número de serviço do host cliente, porque o **`cupsd`** do cliente considera o serviço como concluído assim que ele é encaminhado ao **`cupsd`** do servidor.

Para apagar o serviço de impressão do servidor, use um comando como **`lpstat -h cups.example.com -o`** para determinar o número do serviço no servidor, contanto que o servidor ainda não tenha concluído o serviço de impressão (isto é, não o tenha enviado inteiramente para a impressora). Com esse número, o serviço de impressão pode ser apagado no servidor:

```
cancel -h cups.example.com queue-jobnumber
```

16.8.7 Serviços de impressão com defeito e erros de transferência de dados

Se você desligar a impressora ou encerrar o computador durante o processo de impressão, o serviço de impressão permanecerá na fila. A impressão continua quando o computador (ou a impressora) é ligado novamente. Os serviços de impressão com defeito devem ser removidos da fila com **`cancel`**.

Se o serviço de impressão apresentar defeito ou se ocorrer um erro na comunicação entre o host e a impressora, a impressora imprimirá várias folhas de papel com caracteres ininteligíveis, pois ela não consegue processar os dados corretamente. Para corrigir essa situação, siga as etapas a seguir:

1. Para interromper a impressão, remova todo o papel das bandejas da impressora jato de tinta ou laser. Impressoras de alta qualidade têm um botão de cancelamento da impressão.
2. O serviço de impressão pode ainda estar na fila, já que os serviços apenas são removidos depois de inteiramente enviados à impressora. Use **`lpstat -o`** ou **`lpstat -h cups.example.com -o`** para verificar a fila que está sendo impressa. Apague o serviço de impressão com **`cancel`** *`fila-númerodoserviço`* ou **`cancel -h cups.exemplo.com`** *`fila-númerodoserviço`*.
3. Alguns dados podem ainda ser transferidos à impressora mesmo que o serviço tenha sido apagado da fila. Verifique se há um processo back end do CUPS em execução para a fila respectiva e termine-o.
4. Reinicialize a impressora completamente deixando-a desligada por um tempo. Em seguida, insira o papel e ligue a impressora.

16.8.8 Depurando o CUPS

Use o seguinte procedimento genérico para localizar problemas no CUPS:

1. Defina **`LogLevel debug`** em `/etc/cups/cupsd.conf`.
2. Pare o **`cupsd`**.
3. Remova `/var/log/cups/error_log*` para não precisar procurar em arquivos de registro muito grandes.

4. Inicie o **`cupsd`**.
5. Repita a ação que causou o problema.
6. Verifique as mensagens em `/var/log/cups/error_log*` para identificar a causa do problema.

16.8.9 Para obter mais informações

Há informações detalhadas sobre impressão no SUSE Linux no Banco de Dados de Suporte do openSUSE em http://en.opensuse.org/Portal:Printing. Há soluções para vários problemas específicos no SUSE Knowledgebase (http://www.suse.com/support/). Localize os artigos relevantes com uma pesquisa pelo texto `CUPS`.

17 Gerenciamento dinâmico de dispositivos do Kernel com udev

O kernel pode adicionar ou remover praticamente qualquer dispositivo em um sistema em execução. Mudanças no estado do dispositivo (se um dispositivo foi conectado ou removido) precisam ser propagadas ao espaço do usuário. Os dispositivos deverão ser configurados assim que forem conectados e reconhecidos. Os usuários de um determinado dispositivo precisam ser informados sobre qualquer mudança no estado reconhecido desse dispositivo. O udev fornece a infraestrutura necessária para manter dinamicamente os arquivos dos nós de dispositivo e os links simbólicos no diretório `/dev`. As regras do `udev` fornecem uma maneira de conectar ferramentas externas ao processamento de evento do dispositivo de kernel. Permite personalizar o gerenciamento de dispositivos do `udev`; por exemplo, adicionando determinados scripts para execução como parte do gerenciamento de dispositivos do kernel ou para solicitação e importação de dados adicionais para avaliar durante o gerenciamento de dispositivos.

17.1 O diretório /dev

Os nós de dispositivo no diretório `/dev` fornecem acesso aos dispositivos de kernel correspondentes. Com `udev`, o diretório `/dev` reflete o estado atual do kernel. Cada dispositivo de kernel tem um arquivo de dispositivo correspondente. Se um dispositivo for desconectado do sistema, o nó de dispositivo será removido.

O conteúdo do diretório `/dev` será mantido em um sistema de arquivos temporário, e todos os arquivos serão renderizados a cada inicialização do sistema. Arquivos criados ou modificados manualmente por definição não resistem a uma reinicialização. Diretórios e arquivos estáticos que sempre devem estar presentes no diretório `/dev`, independentemente do estado do dispositivo de kernel correspondente, podem ser criados com systemd-tmpfiles. Os arquivos de configuração estão em `/usr/lib/tmpfiles.d/` e em `/etc/tmpfiles.d/`. Para obter mais informações, consulte a página de manual `systemd-tmpfiles(8)`.

17.2 uevents e udev do Kernel

As informações de dispositivo necessárias são exportadas pelo sistema de arquivos `sysfs`. Para cada dispositivo detectado e inicializado pelo kernel, um diretório com o nome do dispositivo é criado. Ele contém arquivos de atributos com propriedades específicas do dispositivo.

Sempre que um dispositivo é adicionado ou removido, o kernel envia um uevent para notificar o `udev` sobre a mudança. O daemon `udev` lê e analisa todas as regras especificadas nos arquivos `/etc/udev/rules.d/*.rules` uma vez na inicialização e as mantém na memória. Se os arquivos de regras são mudados, adicionados ou removidos, o daemon pode recarregar a representação na memória de todas as regras com o comando **`udevadm control reload_rules`**. Para obter mais detalhes sobre as regras do `udev` e sua sintaxe, consulte a *Seção 17.6, "Influenciando o gerenciamento de eventos de dispositivo do Kernel com as regras do* `udev`*"*.

Cada evento recebido é comparado com o conjunto de regras fornecido. As regras podem adicionar ou modificar chaves de ambiente de eventos, solicitar um nome específico a ser criado pelo nó do dispositivo, adicionar links simbólicos apontando para o nó ou adicionar programas a serem executados após a criação do nó do dispositivo. Os `uevents` de núcleo do driver são recebidos de um soquete netlink do kernel.

17.3 Drivers, módulos de kernel e dispositivos

Os drivers de barramento de kernel pesquisam dispositivos. Para cada dispositivo detectado, o kernel cria uma estrutura de dispositivo interna enquanto o núcleo do driver envia um uevent ao daemon `udev`. Dispositivos de barramento se identificam através de um ID formatado especialmente, que informa o tipo de dispositivo. Geralmente esses IDs consistem em IDs de produto e fornecedor, além de outros valores específicos do subsistema. Cada barramento tem seu próprio esquema para esses IDs, chamados `MODALIAS`. O kernel toma as informações do dispositivo, compõe uma string de ID `MODALIAS` a partir dele e envia essa string junto com o evento. Para um mouse USB, a string tem a seguinte aparência:

```
MODALIAS=usb:v046DpC03Ed2000dc00dsc00dp00ic03isc01ip02
```

Cada driver de dispositivo carrega uma lista de álias conhecidos para os dispositivos que pode tratar. A lista está contida no próprio arquivo de módulo de kernel. O programa depmod lê as listas de ID e cria o arquivo `modules.alias` no diretório `/lib/modules` do kernel para todos os módulos disponíveis atualmente. Com essa infraestrutura, carregar o módulo é fácil

como chamar **modprobe** para cada evento com uma chave MODALIAS. Se **modprobe $MODALIAS** for chamado, ele corresponderá o álias do dispositivo composto para o dispositivo com os álias fornecidos pelos módulos. Se uma entrada correspondente for encontrada, o módulo será carregado. Tudo isso é acionado automaticamente pelo udev.

17.4 Inicialização e configuração do dispositivo inicial

Todos os eventos de dispositivo que ocorrem durante o processo de boot antes da execução do daemon udev são perdidos, pois a infraestrutura para gerenciar esses eventos reside no sistema de arquivos raiz e não está disponível naquele momento. Para cobrir essa perda, o kernel fornece um arquivo uevent localizado no diretório de dispositivo de cada dispositivo no sistema de arquivos sysfs. Ao gravar add para esse arquivo, o kernel envia novamente o mesmo evento como o evento perdido durante a inicialização. Um loop simples em todos os arquivos uevent em /sys aciona todos os eventos novamente para criar os nós de dispositivo e executar a configuração do dispositivo.

Por exemplo, durante o boot, um mouse USB talvez não seja inicializado pela lógica de boot anterior, pois o driver não está disponível nesse momento. O evento para a descoberta do dispositivo foi perdido e não encontrou um módulo de kernel para o dispositivo. Em vez de pesquisar manualmente pelos dispositivos que podem estar conectados, o udev solicita todos os eventos de dispositivo do kernel após a disponibilização do sistema de arquivos raiz, dessa forma, o evento para o dispositivo de mouse USB é executado novamente. Então ele encontra o módulo de kernel no sistema de arquivos raiz montado e o mouse USB pode ser inicializado.

No espaço do usuário, não há diferença visível entre a sequência coldplug do dispositivo e a descoberta de dispositivo durante o tempo de execução. Em ambos os casos, as mesmas regras são usadas para correspondência e os mesmos programas configurados são executados.

17.5 Monitorando o daemon udev em execução

O programa **udevadm monitor** pode ser usado para visualizar os eventos centrais do driver e a temporização dos processos de eventos do udev.

```
UEVENT[1185238505.276660] add   /devices/pci0000:00/0000:00:1d.2/usb3/3-1 (usb)
UDEV  [1185238505.279198] add   /devices/pci0000:00/0000:00:1d.2/usb3/3-1 (usb)
```

```
UEVENT[1185238505.279527] add   /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0
 (usb)
UDEV  [1185238505.285573] add   /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0
 (usb)
UEVENT[1185238505.298878] add   /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/
input/input10 (input)
UDEV  [1185238505.305026] add   /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/
input/input10 (input)
UEVENT[1185238505.305442] add   /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/
input/input10/mouse2 (input)
UEVENT[1185238505.306440] add   /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/
input/input10/event4 (input)
UDEV  [1185238505.325384] add   /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/
input/input10/event4 (input)
UDEV  [1185238505.342257] add   /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/
input/input10/mouse2 (input)
```

As linhas `UEVENT` mostram os eventos que o kernel enviou através de netlink. As linhas `UDEV` mostram os handlers de evento do udev concluídos. _ A temporização é impressa em microssegundos. O tempo entre `UEVENT` e `UDEV` é o tempo que udev levou para processar esse evento ou que o daemon udev atrasou sua execução para sincronizar esse evento com eventos relacionados e já em execução. _ Por exemplo, eventos para partições de disco rígido sempre esperam pela conclusão do evento do dispositivo de disco principal, pois os eventos de partição podem se basear nos dados que o evento de disco principal consultou do hardware.

`udevadm monitor --env` mostra o ambiente de evento completo:

```
ACTION=add
DEVPATH=/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10
SUBSYSTEM=input
SEQNUM=1181
NAME="Logitech USB-PS/2 Optical Mouse"
PHYS="usb-0000:00:1d.2-1/input0"
UNIQ=""
EV=7
KEY=70000 0 0 0 0
REL=103
```

```
MODALIAS=input:b0003v046DpC03Ee0110-e0,1,2,k110,111,112,r0,1,8,amlsfw
```

O `udev` também envia mensagens para o syslog. A prioridade syslog padrão que controla as mensagens que são enviadas ao syslog é especificada no arquivo de configuração do `udev` `/etc/udev/udev.conf`. A prioridade de registro do daemon em execução pode ser modificada com **`udevcontrol log_priority=`***`level/number`*.

17.6 Influenciando o gerenciamento de eventos de dispositivo do Kernel com as regras do udev

Uma regra do `udev` pode corresponder a qualquer propriedade que o kernel adiciona ao evento propriamente dito ou a qualquer informação que o kernel exporta para `sysfs`. A regra também pode solicitar informações adicionais de programas externos. Cada evento é correspondido com as regras fornecidas. Essas regras estão localizadas no diretório `/etc/udev/rules.d`.

Cada linha no arquivo de regras contém pelo menos um par de valores de chave. Há dois tipos de chaves, de atribuição e correspondência. Se todas as chaves de correspondência corresponderem aos valores, a regra será aplicada e as chaves de atribuição serão atribuídas ao valor especificado. Uma regra correspondente pode especificar o nome do nó do dispositivo, adicionar links simbólicos apontando para o nó ou executar um programa especificado como parte do gerenciamento de eventos. Se nenhuma regra de correspondência for encontrada, o nome do nó de dispositivo padrão será usado para criar o nó de dispositivo. As informações detalhadas sobre a sintaxe da regra e as chaves fornecidas para corresponder ou importar os dados estão descritas na página de manual do `udev`. As regras de exemplo a seguir apresentam uma introdução básica à sintaxe da regra do `udev`. As regras de exemplo foram todas tiradas do conjunto de regras padrão do `udev` localizado em `/etc/udev/rules.d/50-udev-default.rules`.

EXEMPLO 17.1 REGRAS DO udev DE EXEMPLO

```
# console
KERNEL=="console", MODE="0600", OPTIONS="last_rule"

# serial devices
KERNEL=="ttyUSB*", ATTRS{product}=="[Pp]alm*Handheld*", SYMLINK+="pilot"
```

```
# printer
SUBSYSTEM=="usb", KERNEL=="lp*", NAME="usb/%k", SYMLINK+="usb%k", GROUP="lp"

# kernel firmware loader
SUBSYSTEM=="firmware", ACTION=="add", RUN+="firmware.sh"
```

A regra do `console` consiste em três chaves: uma chave de correspondência (`KERNEL`) e duas chaves de atribuição (`MODE`, `OPTIONS`). A regra de correspondência `KERNEL` pesquisa qualquer item do tipo `console` na lista de dispositivos. Apenas correspondências exatas são válidas e acionam essa regra para que seja executada. A chave `MODE` atribui permissões especiais ao nó de dispositivo, neste caso, permissões de leitura e gravação apenas ao proprietário desse dispositivo. A chave `OPTIONS` torna esta a última regra a ser aplicada a qualquer dispositivo desse tipo. Qualquer regra posterior que corresponda a esse tipo de dispositivo em particular não terá nenhum efeito.

A regra dos `dispositivos seriais` não está mais disponível em `50-udev-default.rules`, mas ainda vale a pena ser considerada. Consiste em duas chaves de correspondência (`KERNEL` e `ATTRS`) e uma de atribuição (`SYMLINK`). A chave `KERNEL` procura todos os dispositivos do tipo `ttyUSB`. Usando o curinga `*`, essa chave corresponde a diversos desses dispositivos. A segunda chave de correspondência, `ATTRS`, verifica se o arquivo de atribuição do `produto` em `sysfs` para qualquer dispositivo `ttyUSB` contém uma determinada string. A chave de atribuição (`SYMLINK`) aciona a adição de um link simbólico para esse dispositivo em `/dev/pilot`. O operador usado nessa chave (`+=`) diz ao udev para executar essa ação adicionalmente, mesmo se regras anteriores ou posteriores adicionarem outros links simbólicos. _ Como essa regra contém duas chaves de correspondência, ela é aplicada apenas se ambas as condições são cumpridas.

A regra da `impressora` lida com impressoras USB e contém duas chaves de correspondência que devem ser aplicadas para que a regra inteira seja aplicada (`SUBSYSTEM` e `KERNEL`). Três chaves de atribuição lidam com a nomeação desse tipo de dispositivo (`NAME`), a criação dos links de dispositivo simbólicos (`SYMLINK`) e a participação no grupo desse tipo de dispositivo (`GROUP`). O uso do curinga `*` na chave `KERNEL` faz com que ela corresponda a diversos dispositivos de impressora `lp`. Substituições são usadas pelo nome do dispositivo interno tanto na chave `NAME` quanto na `SYMLINK` para estender essas strings. Por exemplo, o link simbólico para a primeira impressora USB `lp` seria `/dev/usblp0`.

A regra do `carregador de firmware do kernel` faz o udev carregar firmware adicional por um script de assistente externo durante o tempo de execução. A chave de correspondência `SUBSYSTEM` procura o subsistema de `firmware`. A chave `ACTION` verifica se algum dispositivo pertencente ao subsistema de `firmware` foi adicionado. A chave `RUN+=` aciona a execução do script `firmware.sh` para localizar o firmware a ser carregado.

Algumas características são comuns a todas as regras:

- Cada regra é composta por um ou mais pares de valores de chaves separados por vírgula.
- A operação de uma chave é determinada pelo operador. As regras do `udev` suportam diversos operadores diferentes.
- Cada valor dado deve estar entre aspas.
- Cada linha do arquivo de regras representa uma regra. Se a regra for maior do que uma linha, use `\` para unir as linhas diferentes como se faz na sintaxe do shell.
- As regras do udev suportam um padrão no estilo do shell que corresponde aos padrões de `*`, `?` e `[]`.
- As regras do `udev` suportam substituições.

17.6.1 Usando operadores nas regras do udev

Ao criar chaves, você pode escolher dentre diversos operadores diferentes, dependendo do tipo de chave que quiser criar. Normalmente, as chaves de correspondência são usadas para localizar um valor que corresponda ou explicitamente não corresponda ao valor da pesquisa. As chaves de correspondência contêm um dos seguintes operadores:

`==`

Comparar para igualdade. Se a chave contém um padrão de pesquisa, todos os resultados correspondentes a esse padrão são válidos.

`!=`

Comparar para não igualdade. Se a chave contém um padrão de pesquisa, todos os resultados correspondentes a esse padrão são válidos.

Qualquer um dos operadores a seguir também pode ser usado com chaves de atribuição:

`=`
: Atribuir um valor a uma chave. Se a chave consistia anteriormente em uma lista de valores, ela é redefinida e apenas o valor único é atribuído.

`+=`
: Adicionar um valor a uma chave que contenha uma lista de entradas.

`:=`
: Atribuir um valor final. Não permitir nenhuma mudança posterior por regras posteriores.

17.6.2 Usando substituições nas regras do udev

As regras do `udev` suportam o uso de marcadores e substituições. Use-as como faria em qualquer outro script. É possível usar as seguintes substituições com as regras do `udev`:

`%r`, `$root`
: O diretório do dispositivo, `/dev` por padrão.

`%p`, `$devpath`
: O valor de `DEVPATH`.

`%k`, `$kernel`
: O valor de `KERNEL` ou o nome do dispositivo interno.

`%n`, `$number`
: O nome do dispositivo.

`%N`, `$tempnode`
: O nome temporário do arquivo de dispositivo.

`%M`, `$major`
: O número maior do dispositivo.

`%m`, `$minor`
: O número menor do dispositivo.

`%s{`*`attribute`*`}`, `$attr{`*`attribute`*`}`
: O valor de um atributo `sysfs` (especificado por *`attribute`*).

`%E{variable}`, `$attr{variable}`

O valor de uma variável do ambiente (especificado por *`variable`*).

`%c`, `$result`

A saída de `PROGRAM`.

`%%`

O caractere `%`.

`$$`

O caractere `$`.

17.6.3 Usando as chaves de correspondência do udev

As chaves de correspondência descrevem as condições que devem ser atendidas para aplicar uma regra do `udev`. As seguintes chaves de correspondência estão disponíveis:

`ACTION`

O nome da ação do evento, por exemplo, `add` ou `remove` na adição ou remoção de um dispositivo.

`DEVPATH`

O caminho do dispositivo do evento, por exemplo, `DEVPATH=/bus/pci/drivers/ipw3945` para procurar todos os eventos relacionados ao driver ipw3945.

`KERNEL`

O nome interno (do kernel) do dispositivo do evento.

`SUBSYSTEM`

O subsistema do dispositivo do evento, por exemplo, `SUBSYSTEM=usb` para todos os eventos relacionados a dispositivos USB.

`ATTR{`*`nome de arquivo`*`}`

Atributos `sysfs` do dispositivo do evento. Para corresponder a uma string contida no nome de arquivo do atributo `vendor`, você poderia usar `ATTR{vendor}=="On[sS]tream"`, por exemplo.

`KERNELS`

Permitem que o `udev` pesquise o caminho do dispositivo para encontrar um nome de dispositivo correspondente.

`SUBSYSTEMS`

Permitem que o `udev` pesquise o caminho do dispositivo para encontrar um nome de subsistema do dispositivo correspondente.

`DRIVERS`

Permitem que o `udev` pesquise o caminho do dispositivo para encontrar um nome de driver do dispositivo correspondente.

`ATTRS{`*`nome de arquivo`*`}`

Permitem que o `udev` pesquise o caminho do dispositivo para encontrar um com valores de atributo `sysfs` correspondentes.

`ENV{`*`chave`*`}`

O valor de uma variável de ambiente, por exemplo, `ENV{ID_BUS}="ieee1394` para procurar todos os eventos relacionados ao ID do barramento FireWire.

`PROGRAM`

Permite que o `udev` execute um programa externo. Para ser bem-sucedido, o programa deve retornar com código de saída zero. A saída do programa, impressa em STDOUT, está disponível para a chave `RESULT`.

`RESULT`

Corresponder à string de saída da última chamada de `PROGRAM`. Incluir esta chave na mesma regra que a chave `PROGRAM` ou em uma posterior.

17.6.4 Usando as chaves de atribuição do udev

Em contraste com as chaves de correspondência descritas anteriormente, as chaves de atribuição não descrevem condições que devem ser cumpridas. Elas atribuem valores, nomes e ações aos nós do dispositivo mantidos pelo `udev`.

`NAME`

O nome do nó de dispositivo a ser criado. Depois que uma regra definir o nome de um nó, todas as outras regras com a chave `NAME` referente a esse nó serão ignoradas.

`SYMLINK`

O nome de um link simbólico relacionado ao nó a ser criado. Várias regras de correspondência podem adicionar links simbólicos a serem criados com o nó do dispositivo. Você também pode especificar vários links simbólicos para um nó em uma regra usando o caractere de espaço para separar os nomes dos links simbólicos.

`OWNER, GROUP, MODE`

As permissões do novo nó de dispositivo. Os valores especificados aqui sobregravam qualquer coisa que tenha sido compilada.

`ATTR{`*`chave`*`}`

Especifica um valor para ser gravado no atributo `sysfs` do dispositivo de evento. Se o operador `==` é usado, essa chave também é usada para corresponder com o valor de um atributo sysfs.

`ENV{`*`chave`*`}`

Indica ao `udev` para exportar uma variável para o ambiente. Se o operador `==` é usado, essa chave também é usada para corresponder com uma variável de ambiente.

`RUN`

Indica ao `udev` para adicionar um programa à lista de programas a serem executados neste dispositivo. Lembre-se de restringir isso a tarefas muito curtas, a fim de evitar o bloqueio de outros eventos para esse dispositivo.

`LABEL`

Adicionar um rótulo para onde um `GOTO` possa ir.

`GOTO`

Indica ao `udev` para ignorar uma quantidade de regras e continuar com uma que inclua o rótulo citado pela chave `GOTO`.

`IMPORT{`*`tipo`*`}`

Carregar variáveis para o ambiente do evento, como a saída de um programa externo. O `udev` importa variáveis de vários tipos diferentes. Se nenhum tipo for especificado, o `udev` tentará determinar o tipo sozinho, com base na parte executável das permissões do arquivo.

- `program` diz ao `udev` para executar um programa externo e importar sua saída.
- `file` diz ao `udev` para importar um arquivo texto.
- `parent` diz ao `udev` para importar as chaves armazenadas do dispositivo pai.

`WAIT_FOR_SYSFS`

Indica ao `udev` para aguardar a criação do arquivo `sysfs` especificado para determinado dispositivo. Por exemplo, `WAIT_FOR_SYSFS="ioerr_cnt"` informa o udev para aguardar até que o arquivo `ioerr_cnt` seja criado.

`OPTIONS`

A chave `OPTION` pode ter diversos valores possíveis:

- `last_rule` diz ao `udev` para ignorar todas as regras posteriores.
- `ignore_device` diz ao `udev` para ignorar esse evento completamente.
- `ignore_remove` diz ao `udev` para ignorar todos os eventos de remoção posteriores para o dispositivo.
- `all_partitions` diz ao `udev` para criar nós de dispositivo para todas as partições disponíveis em um dispositivo de bloco.

17.7 Nomeação de dispositivo persistente

O diretório do dispositivo dinâmico e a infraestrutura de regras do `udev` possibilitam especificar nomes estáveis para todos os dispositivos de disco, independentemente da ordem de reconhecimento ou da conexão usada para o dispositivo. Cada dispositivo de bloco apropriado criado pelo kernel é examinado por ferramentas com conhecimento especial sobre determinados barramentos, tipos de unidade ou sistemas de arquivos. Com o nome do nó do dispositivo fornecido pelo kernel dinâmico, o `udev` mantém as classes de links persistentes apontando para o dispositivo:

```
/dev/disk
|-- by-id
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B -> ../../sda
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part1 -> ../../sda1
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part6 -> ../../sda6
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part7 -> ../../sda7
|   |-- usb-Generic_STORAGE_DEVICE_02773 -> ../../sdd
|   `-- usb-Generic_STORAGE_DEVICE_02773-part1 -> ../../sdd1
|-- by-label
|   |-- Photos -> ../../sdd1
|   |-- SUSE10 -> ../../sda7
|   `-- devel -> ../../sda6
|-- by-path
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0 -> ../../sda
```

```
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part1 -> ../../sda1
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part6 -> ../../sda6
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part7 -> ../../sda7
|   |-- pci-0000:00:1f.2-scsi-1:0:0:0 -> ../../sr0
|   |-- usb-02773:0:0:2 -> ../../sdd
|   |-- usb-02773:0:0:2-part1 -> ../../sdd1
`-- by-uuid
    |-- 159a47a4-e6e6-40be-a757-a629991479ae -> ../../sda7
    |-- 3e999973-00c9-4917-9442-b7633bd95b9e -> ../../sda6
    `-- 4210-8F8C -> ../../sdd1
```

17.8 Arquivos usados pelo udev

`/sys/*`
: Sistema de arquivos virtual fornecido pelo kernel do Linux, exportando todos os dispositivos conhecidos atualmente. Essas informações são usadas pelo `udev` para criar nós de dispositivo em `/dev`

`/dev/*`
: Nós de dispositivo criados dinamicamente e conteúdo estático criado com systemd-tmpfiles. Para obter mais informações, consulte a página de manual `systemd-tmpfiles(8)`.

Os arquivos e os diretórios a seguir incluem elementos cruciais da infraestrutura do `udev`:

`/etc/udev/udev.conf`
: Arquivo de configuração principal do `udev`.

`/etc/udev/rules.d/*`
: Regras de correspondência de evento do `udev`.

`/usr/lib/tmpfiles.d/` e `/etc/tmpfiles.d/`
: Responsáveis pelo conteúdo do `/dev` estático.

`/usr/lib/udev/*`
: Programas ajudantes chamados de regras do `udev`.

17.9 Para obter mais informações

Para obter mais informações sobre a infraestrutura do `udev`, consulte as seguintes páginas de manual:

`udev`

Informações importantes sobre `udev`, chaves, regras e outras questões essenciais de configuração.

`udevadm`

É possível usar o **`udevadm`** para controlar o comportamento de tempo de execução do `udev`, solicitar eventos do kernel, gerenciar a fila de eventos e fornecer mecanismos simples de depuração.

`udevd`

Informações sobre o daemon de gerenciamento de eventos do `udev`.

18 O sistema X Window

O X Window System (X11) é o padrão de fato para interfaces gráficas do usuário no Unix. O X é baseado em rede, permitindo que aplicativos iniciados em um host sejam exibidos em outro host conectado em qualquer tipo de rede (LAN ou Internet). Este capítulo apresenta informações básicas sobre a configuração do X e explica como usar as fontes no SUSE® Linux Enterprise Desktop.

Na maioria dos casos, o X Window System não precisa de nenhuma configuração. O hardware é detectado dinamicamente durante a inicialização do X. Portanto, o uso do `xorg.conf` foi descontinuado. Se você ainda tiver que especificar opções personalizadas para mudar o comportamento do X, poderá modificar os arquivos de configuração em `/etc/X11/xorg.conf.d/`.

18.1 Instalando e configurando fontes

É possível categorizar as fontes no Linux em duas partes:

Fontes geométricas ou vetoriais

Apresenta uma descrição matemática; por exemplo, instruções sobre como desenhar a forma de um glifo. Dessa forma, cada glifo pode ser dimensionado a tamanhos arbitrários sem perder a qualidade. Antes de usar a fonte (ou glifo), as descrições matemáticas devem ser transformadas em raster (grade). Este processo é denominado *rasterização de fonte*. As *dicas de fonte* (embutidas na fonte) melhoram e otimizam o resultado da renderização de determinado tamanho. A rasterização e as dicas são feitas com a biblioteca FreeType.

Os formatos comuns no Linux são PostScript Type 1 e Type 2, TrueType e OpenType.

Fontes de bitmap ou raster

Compostas por uma matriz de pixels designados para um tamanho de fonte específico. As fontes de bitmap são extremamente rápidas e simples de se renderizar. Porém, em comparação com as fontes vetoriais, as fontes de bitmap não podem ser dimensionadas sem perda de qualidade. Sendo assim, essas fontes são normalmente distribuídas em tamanhos diferentes. Atualmente, as fontes de bitmap ainda são usadas no console do Linux e, algumas vezes, em terminais.

No Linux, o Portable Compiled Format (PCF) ou Glyph Bitmap Distribution Format (BDF) são os formatos mais comuns.

A aparência dessas fontes pode ser influenciada por dois aspectos principais:

- a escolha de uma família de fontes adequada e
- a renderização da fonte com um algoritmo que atinja resultados agradáveis aos olhos do receptor.

O último ponto só será relevante no caso de fontes vetoriais. Embora os dois pontos acima sejam altamente subjetivos, alguns padrões devem ser criados.

Os sistemas de renderização de fonte do Linux são compostos por várias bibliotecas com relações diferentes. A biblioteca básica de renderização de fonte é a FreeType (http://www.freetype.org/), que converte glifos de fonte de formatos suportados em glifos de bitmap otimizados. O processo de renderização é controlado por um algoritmo e seus parâmetros (que podem estar sujeitos a questões de patente).

Cada programa ou biblioteca que usa FreeType deve consultar a biblioteca Fontconfig (http://www.fontconfig.org/). Essa biblioteca combina a configuração da fonte dos usuários e do sistema. Quando um usuário altera a configuração de Fontconfig, essa alteração resulta em aplicativos compatíveis com Fontconfig.

A forma OpenType mais sofisticada, necessária para scripts como Arabic, Han ou Phags-Pa e outro tipo de processamento de texto de nível mais elevado, fica sob a responsabilidade de Harfbuzz (http://www.harfbuzz.org/) ou Pango (http://www.pango.org/), para citar alguns exemplos.

18.1.1 Mostrando as fontes instaladas

Para ter uma visão geral sobre as fontes que estão instaladas no sistema, execute os comandos **`rpm`** ou **`fc-list`**. Os dois apresentam uma boa resposta, mas podem retornar uma lista diferente, dependendo do sistema e da configuração do usuário:

`rpm`

Chame **`rpm`** para ver quais pacotes de software com fontes estão instalados no sistema:

```
rpm -qa '*fonts*'
```

Cada pacote de fontes deve satisfazer essa expressão. No entanto, o comando pode retornar alguns falsos positivos, como `fonts-config` (que não é uma fonte e nem inclui fontes).

`fc-list`

Chame **`fc-list`** para ter uma visão geral sobre as famílias de fontes que podem ser acessadas e saber se elas estão instaladas no sistema ou no diretório pessoal:

```
fc-list ':' family
```

Nota: Comando `fc-list`

O comando **`fc-list`** é um agrupador da biblioteca Fontconfig. É possível consultar uma variedade de informações interessantes do Fontconfig ou, para ser mais preciso, de seu cache. Consulte **`man 1 fc-list`** para obter mais detalhes.

18.1.2 Vendo fontes

Informações sobre
, consulte

Para saber a aparência de uma família de fontes instalada, use o comando **`ftview`** (pacote `ft2demos`) ou visite http://fontinfo.opensuse.org/. Por exemplo, para exibir a fonte FreeMono no ponto 14, use **`ftview`** da seguinte forma:

```
ftview 14 /usr/share/fonts/truetype/FreeMono.ttf
```

Se precisar de mais informações, acesse http://fontinfo.opensuse.org/ para saber quais estilos (regular, negrito, itálico, etc.) e linguagens são suportados.

18.1.3 Consultando fontes

Para consultar a fonte que será usada quando determinado padrão for especificado, use o comando **`fc-match`**.

Por exemplo, se o padrão já tiver uma fonte instalada, o **`fc-match`** retornará o nome do arquivo, a família de fontes e o estilo:

```
tux > fc-match 'Liberation Serif'
LiberationSerif-Regular.ttf: "Liberation Serif" "Regular"
```

Se a fonte desejada não existir no sistema, as regras de correspondência da Fontconfig serão aplicadas para tentar encontrar as fontes disponíveis mais parecidas. Ou seja, a sua solicitação é substituída:

```
tux > fc-match 'Foo Family'
DejaVuSans.ttf: "DejaVu Sans" "Book"
```

A Fontconfig suporta *áliases*: um nome é substituído por outro nome de família. Um exemplo comum é com nomes genéricos, como “sans-serif”, “serif” e “monospace”. Esses nomes de álias podem ser substituídos por nomes reais de família ou até mesmo por uma lista preferencial de nomes de família:

```
tux > for font in serif sans mono; do fc-match "$font" ; done
DejaVuSerif.ttf: "DejaVu Serif" "Book"
DejaVuSans.ttf: "DejaVu Sans" "Book"
DejaVuSansMono.ttf: "DejaVu Sans Mono" "Book"
```

O resultado pode variar no sistema de acordo com as fontes que estão instaladas.

Nota: Regras de similaridade segundo a Fontconfig

A Fontconfig *sempre* retorna uma família real (se pelo menos uma estiver instalada) de acordo com a solicitação especificada, a mais parecida possível. A “similaridade” depende das métricas internas da Fontconfig e das configurações de usuário ou administrador da Fontconfig.

18.1.4 Instalando fontes

Para instalar uma nova fonte, os seguintes métodos principais estão disponíveis:

1. Instalar manualmente os arquivos de fonte, como `*.ttf` ou `*.otf`, em um diretório de fontes conhecido. Se precisar ser um diretório de todo o sistema, use o padrão `/usr/share/fonts`. Para instalação em seu diretório pessoal, use `~/.config/fonts`.

Para sair dos padrões, a Fontconfig permite escolher um diretório diferente. Informe a Fontconfig usando o elemento `<dir>`. Consulte a *Seção 18.1.5.2, "Conhecendo o XML da Fontconfig"* para obter os detalhes.

2. Instalar as fontes usando o **`zypper`**. Muitas fontes já estão disponíveis como um pacote, seja em sua distribuição do SUSE ou no repositório M17N:fonts (http://download.opensuse.org/repositories/M17N:/fonts/). Adicione o repositório à sua lista usando o seguinte comando. Por exemplo, para adicionar um repositório para o SLE 12:

```
sudo zypper ar
     http://download.opensuse.org/repositories/M17N:/fonts/SLE_12/
M17N:fonts.repo
```

Para procurar o *`NOME_DA_FAMÍLIA_DE_FONTES`* use este comando:

```
sudo zypper se 'FONT_FAMILY_NAME*fonts'
```

18.1.5 Configurando a aparência das fontes

Dependendo do meio de renderização e do tamanho da fonte, o resultado pode não ser satisfatório. Por exemplo, um monitor médio atual possui resolução de 100 dpi que torna os pixels grandes demais e os glifos pesados.

Há diversos algoritmos disponíveis para lidar com resoluções baixas, como suavização (atenuação da escala de cinzas), dicas (ajuste à grade) ou renderização de subpixel (triplicação da resolução em uma direção). Esses algoritmos também podem ser diferentes entre um formato de fonte e outro.

Importante: Questões de patentes com a renderização de subpixel

A renderização de subpixel não é usada em distribuições do SUSE. Embora a FreeType2 suporte esse algoritmo, ele envolve várias patentes que vencem no fim do ano de 2019. Portanto, a configuração das opções de renderização de subpixel na Fontconfig não terá nenhum efeito, exceto se o sistema tiver a biblioteca FreeType2 com a renderização de subpixel compilada.

Pela Fontconfig, é possível selecionar um algoritmo de renderização para cada fonte separadamente ou para um conjunto de fontes.

18.1.5.1 Configurando fontes pelo `sysconfig`

O SUSE Linux Enterprise Desktop vem com uma camada do `sysconfig` acima do Fontconfig. Este é um ótimo ponto de partida para testar a configuração da fonte. Para mudar as configurações padrão, edite o arquivo de configuração `/etc/sysconfig/fonts-config`. (ou use o módulo sysconfig do YaST). Após editar o arquivo, execute **`fonts-config`**:

```
sudo /usr/sbin/fonts-config
```

Reinicie o aplicativo para tornar o efeito visível. Lembre-se das seguintes questões:

- Alguns aplicativos precisam ser reiniciados. Por exemplo, o Firefox sempre lê a configuração de Fontconfig de tempos em tempos. As guias recém-criadas ou recarregadas acessam as novas configurações de fontes posteriormente.
- O script **`fonts-config`** é chamado automaticamente após cada instalação ou remoção de pacote (do contrário, trata-se de um bug do pacote de software de fontes).
- Cada variável sysconfig pode ser temporariamente anulada e substituída pela opção de linha de comando **`fonts-config`**. Consulte **`fonts-config --help`** para obter os detalhes.

Há diversas variáveis sysconfig que podem ser alteradas. Consulte **`man 1 fonts-config`** ou a página de ajuda do módulo sysconfig do YaST. As seguintes variáveis são alguns exemplos:

Uso de algoritmos de renderização

Considere `FORCE_HINTSTYLE`, `FORCE_AUTOHINT`, `FORCE_BW`, `FORCE_BW_MONOSPACE`, `USE_EMBEDDED_BITMAPS` e `EMBEDDED_BITMAP_LANGAGES`

Listas preferenciais de áliases genéricos

Uso `PREFER_SANS_FAMILIES`, `PREFER_SERIF_FAMILIES`, `PREFER_MONO_FAMILIES` e `SEARCH_METRIC_COMPATIBLE`

A lista a seguir mostra alguns exemplos de configuração, começando das fontes “mais legíveis” (mais contraste) até as fontes “mais bonitas” (mais suavizadas).

Fontes de bitmap

Prefira as fontes de bitmap usando as variáveis `PREFER_*_FAMILIES` . Siga o exemplo na seção de Ajuda dessas variáveis. Observe que essas fontes são renderizadas em preto e branco, e não suavizadas, e que as fontes de bitmap estão disponíveis em vários tamanhos. Considere usar

```
SEARCH_METRIC_COMPATIBLE="no"
```

para desabilitar as substituições de nome de família orientadas por compatibilidade de métrica.

Fontes escaláveis renderizadas em preto e branco

As fontes escaláveis renderizadas sem suavização podem produzir resultados parecidos com as fontes de bitmap, enquanto mantêm a escalabilidade da fonte. Use fontes com dicas bem elaboradas, como as famílias Liberation. Não há muitas opções de fontes com dicas bem elaboradas. Defina a seguinte variável para forçar este método:

```
FORCE_BW="yes"
```

Fontes monoespaçadas renderizadas em preto e branco

Somente renderize fontes monoespaçadas sem suavização, do contrário, use as configurações padrão:

```
FORCE_BW_MONOSPACE="yes"
```

Configurações Padrão

Todas as fontes são renderizadas com suavização. As fontes com dicas bem elaboradas serão renderizadas com o BCI (*byte code interpreter* — intérprete de código de byte), e o restante com o autohinter (`hintstyle=hintslight`). Deixe todas as variáveis sysconfig relevantes com a configuração padrão.

Fontes CFF

Use as fontes no formato CFF. Elas também podem ser consideradas mais legíveis do que as fontes TrueType padrão, por causa das atuais melhorias na FreeType2. Faça um teste com elas seguindo o exemplo de `PREFER_*_FAMILIES`. É possível torná-las mais escuras e colocá-las em negrito com:

```
SEARCH_METRIC_COMPATIBLE="no"
```

já que são renderizadas por `hintstyle=hintslight`, por padrão. Considere usar também:

```
SEARCH_METRIC_COMPATIBLE="no"
```

Autohinter exclusivamente

Mesmo para uma fonte com dicas bem elaboradas, use o autohinter da FreeType2. Ele pode gerar um resultado mais espesso com contraste menor e, às vezes, um pouco mais difuso. Defina a seguinte variável para ativá-lo:

```
FORCE_AUTOHINTER="yes"
```

Use `FORCE_HINTSTYLE` para controlar o nível de dicas.

18.1.5.2 Conhecendo o XML da Fontconfig

O formato de configuração da Fontconfig é o *eXtensible Markup Language* (XML). Estes exemplos não são uma referência completa, e sim uma visão geral. Você encontra detalhes e outras inspirações no **`man 5 fonts-conf`** ou em `/etc/fonts/conf.d/`.

O arquivo de configuração central do Fontconfig é `/etc/fonts/fonts.conf`, que, além de outras coisas, inclui todo o diretório `/etc/fonts/conf.d/`. Para personalizar a Fontconfig, há dois lugares para você fazer as mudanças:

ARQUIVOS DE CONFIGURAÇÃO DA FONTCONFIG

1. **Mudanças de todo o sistema.** Edite o arquivo `/etc/fonts/local.conf` (por padrão, ele inclui um elemento `fontconfig` vazio).

2. **Mudanças específicas do usuário.** Edite o arquivo `~/.config/fontconfig/fonts.conf`. Coloque os arquivos de configuração da Fontconfig no diretório `~/.config/fontconfig/conf.d/`.

As mudanças específicas do usuário sobregravam qualquer configuração de todo o sistema.

Nota: Arquivo de configuração do usuário descontinuado

O arquivo `~/.fonts.conf` está marcado como descontinuado e não deve mais ser usado. Use agora o `~/.config/fontconfig/fonts.conf`.

Cada arquivo de configuração precisa ter um elemento `fontconfig`. Dessa forma, o arquivo mínimo terá a seguinte aparência:

```
<?xml version="1.0"?>
   <!DOCTYPE fontconfig SYSTEM "fonts.dtd">
   <fontconfig>
   <!-- Insert your changes here -->
   </fontconfig>
```

Se os diretórios padrão não forem suficientes, insira o elemento `dir` com o respectivo diretório:

```
<dir>/usr/share/fonts2</dir>
```

A Fontconfig procura as fontes *repetidamente*.

É possível escolher os algoritmos de renderização de fonte com o seguinte trecho da Fontconfig (consulte o *Exemplo 18.1, "Especificando algoritmos de renderização"*):

EXEMPLO 18.1 ESPECIFICANDO ALGORITMOS DE RENDERIZAÇÃO

```
<match target="font">
 <test name="family">
  <string>FAMILY_NAME</string>
 </test>
 <edit name="antialias" mode="assign">
  <bool>true</bool>
 </edit>
 <edit name="hinting" mode="assign">
  <bool>true</bool>
 </edit>
 <edit name="autohint" mode="assign">
  <bool>false</bool>
 </edit>
 <edit name="hintstyle" mode="assign">
  <const>hintfull</const>
 </edit>
</match>
```

É possível testar várias propriedades de fontes. Por exemplo, o elemento `<test>` pode testar a família de fontes (conforme mostrado no exemplo), o intervalo de tamanhos, o espaçamento, o formato da fonte, etc. Quando `<test>` é completamente abandonado, todos os elementos `<edit>` são aplicados a cada fonte (mudança global).

EXEMPLO 18.2 SUBSTITUIÇÕES DE ÁLIAS E NOME DE FAMÍLIA

Regra 1

```
<alias>
 <family>Alegreya SC</family>
 <default>
  <family>serif</family>
 </default>
</alias>
```

Regra 2

```
<alias>
 <family>serif</family>
 <prefer>
  <family>Droid Serif</family>
 </prefer>
</alias>
```

Regra 3

```
<alias>
 <family>serif</family>
 <accept>
  <family>STIXGeneral</family>
 </accept>
</alias>
```

As regras do *Exemplo 18.2, "Substituições de álias e nome de família"* criam uma PFL (*prioritized family list* — lista prioritária de famílias). Dependendo do elemento, são executadas ações diferentes:

`<default>` da ***Regra 1***

Esta regra adiciona um nome da família `serif` *ao fim* da PFL.

`<prefer>` da *Regra 2*

Esta regra adiciona “Droid Serif” *logo antes da* primeira ocorrência de `serif` na PFL, sempre que `Alegreya SC` estiver presente na PFL.

`<accept>` da *Regra 3*

Esta regra adiciona o nome da família “STIXGeneral” *logo depois da* primeira ocorrência do nome da família `serif` na PFL.

Juntando tudo isso, quando os trechos ocorrem na ordem *Regra 1*, *Regra 2* e *Regra 3* e o usuário solicita “Alegreya SC”, a PFL é criada conforme mostrado na *Tabela 18.1, “Gerando a PFL com base nas regras de Fontconfig”*.

TABELA 18.1 GERANDO A PFL COM BASE NAS REGRAS DE FONTCONFIG

Ordem	PFL atual
Solicitação	`Alegreya SC`
Regra 1	`Alegreya SC`, `serif`
Regra 2	`Alegreya SC`, `Droid Serif`, `serif`
Regra 3	`Alegreya SC`, `Droid Serif`, `serif`, `STIXGeneral`

Nas métricas da Fontconfig, o nome da família tem maior prioridade sobre os outros padrões, como estilo, tamanho, etc. A Fontconfig verifica qual família está instalada no sistema. Se “Alegreya SC” estiver instalada, a Fontconfig a retornará. Do contrário, ela solicitará “Droid Serif”, etc.

Tenha cuidado. Quando a ordem dos trechos da Fontconfig é modificada, a Fontconfig poderá retornar resultados diferentes, conforme mostrado na *Tabela 18.2, “Resultados da geração da PFL com base nas regras da Fontconfig com a ordem modificada”*.

TABELA 18.2 RESULTADOS DA GERAÇÃO DA PFL COM BASE NAS REGRAS DA FONTCONFIG COM A ORDEM MODIFICADA

Ordem	PFL atual	Nota
Solicitação	`Alegreya SC`	Mesma solicitação efetuada.
Regra 2	`Alegreya SC`	`serif` não está na PFL; nada é substituído

Ordem	PFL atual	Nota
Regra 3	`Alegreya SC`	`serif` não está na PFL; nada é substituído
Regra 1	`Alegreya SC`, `serif`	`Alegreya SC` presente na PFL; a substituição é realizada

Nota: Implicação.

Pense no álias `<default>` como uma classificação ou inclusão deste grupo (se não estiver instalado). Conforme mostrado no exemplo, `<default>` sempre deve preceder os áliases `<prefer>` e `<accept>` deste grupo.

A classificação `<default>` não se limita aos áliases genéricos serif, sans-serif e monospace. Consulte `/usr/share/fontconfig/conf.avail/30-metric-aliases.conf` para ver um exemplo complexo.

O seguinte trecho da Fontconfig no *Exemplo 18.3, "Substituições de álias e nome de família"* cria um grupo `serif`. Cada família desse grupo poderá substituir outras famílias, caso ainda não exista uma fonte instalada.

EXEMPLO 18.3 SUBSTITUIÇÕES DE ÁLIAS E NOME DE FAMÍLIA

```
<alias>
 <family>Alegreya SC</family>
 <default>
  <family>serif</family>
 </default>
</alias>
<alias>
 <family>Droid Serif</family>
 <default>
  <family>serif</family>
 </default>
</alias>
<alias>
```

```
 <family>STIXGeneral</family>
 <default>
  <family>serif</family>
 </default>
</alias>
<alias>
 <family>serif</family>
 <accept>
  <family>Droid Serif</family>
  <family>STIXGeneral</family>
  <family>Alegreya SC</family>
 </accept>
</alias>
```

A prioridade é aplicada seguindo a ordem do álias `<accept>`. Da mesma forma, é possível usar os áliases `<prefer>` mais fortes.

O *Exemplo 18.2, "Substituições de álias e nome de família"* é expandido pelo *Exemplo 18.4, "Substituições de álias e nome de família"*.

EXEMPLO 18.4 SUBSTITUIÇÕES DE ÁLIAS E NOME DE FAMÍLIA

Regra 4

```
<alias>
 <family>serif</family>
 <accept>
  <family>Liberation Serif</family>
 </accept>
</alias>
```

Regra 5

```
<alias>
 <family>serif</family>
 <prefer>
  <family>DejaVu Serif</family>
 </prefer>
</alias>
```

A configuração expandida do *Exemplo 18.4, "Substituições de álias e nome de família"* leva à seguinte evolução da PFL:

TABELA 18.3 RESULTADOS DA GERAÇÃO DA PFL COM BASE NAS REGRAS DE FONTCONFIG

Ordem	PFL atual
Solicitação	`Alegreya SC`
Regra 1	`Alegreya SC`, `serif`
Regra 2	`Alegreya SC`, `Droid Serif`, `serif`
Regra 3	`Alegreya SC`, `Droid Serif`, `serif`, `STIXGeneral`
Regra 4	`Alegreya SC`, `Droid Serif`, `serif`, `Liberation Serif`, `STIXGeneral`
Regra 5	`Alegreya SC`, `Droid Serif`, `DejaVu Serif`, `serif`, `Liberation Serif`, `STIXGeneral`

Nota: Implicações.

- Caso haja várias declarações `<accept>` para o mesmo nome genérico, a declaração que for analisada por último "vencerá". Se possível, não use `<accept>` **após** o usuário (`/etc/fonts/conf.d/*-user.conf`) ao criar uma configuração de todo o sistema.

- Caso haja várias declarações `<prefer>` para o mesmo nome genérico, a declaração que for analisada por último "vencerá". Se possível, não use `<prefer>` **antes** do usuário na configuração de todo o sistema.

- Cada declaração `<prefer>` sobregrava as declarações `<accept>` para o mesmo nome genérico. Se o administrador quiser dar ao usuário liberdade total para utilizar `<accept>`, e não apenas `<prefer>`, ele não deverá usar `<prefer>` na configuração de todo o sistema. Por outro lado, os usuários utilizam mais o `<prefer>`, portanto, isso não pode ser restritivo, já que constatamos também o uso de `<prefer>` nas configurações de todo o sistema.

18.2 Para obter mais informações

Instale os pacotes `xorg-docs` para obter informações mais detalhadas sobre o X11. O **`man 5 xorg.conf`** apresenta mais informações sobre o formato da configuração manual (se necessário). Mais informações sobre o desenvolvimento do X11 podem ser encontradas na home page do projeto, em http://www.x.org.

Os drivers estão nos pacotes `xf86-video-*`, por exemplo `xf86-video-nv`. Muitos dos drivers incluídos nesses pacotes estão descritos em detalhes na página de manual relacionada. Por exemplo, se você usar o driver `nv`, encontre mais informações sobre ele em **`man 4 nv`**.

Informações sobre drivers de terceiros devem estar disponíveis em `/usr/share/doc/packages/<nome_do_pacote>`. Por exemplo, a documentação de `x11-video-nvidiaG03` está disponível em `/usr/share/doc/packages/x11-video-nvidiaG03` após a instalação do pacote.

19 Acessando sistemas de arquivos com o FUSE

FUSE é o acrônimo de *file system in userspace* (sistema de arquivos no espaço do usuário). Isso significa que você pode configurar e montar um sistema de arquivos como um usuário sem privilégios. Normalmente, você precisa ser o `root` para executar esta tarefa. O FUSE, isoladamente, é um módulo de kernel. Combinado-o a plug-ins, você pode estender o FUSE para acessar quase todos os sistemas de arquivos, como conexões SSH remotas, imagens ISO e muito mais..

19.1 Configurando o FUSE

Antes de usar o FUSE, é necessário instalar o pacote `fuse`. Dependendo do sistema de arquivos que você deseja usar, serão necessários plug-ins adicionais, disponíveis em pacotes separados. Os plug-ins do FUSE não estão incluídos no SUSE Linux Enterprise.

Em geral, não é necessário configurar o FUSE, basta usá-lo. Mas vale a pena criar um diretório com todos os pontos de montagem combinados. Por exemplo, você pode criar um diretório `~/mounts` e inserir nele subdiretórios para os diferentes sistemas de arquivo.

19.2 Plug-ins disponíveis do FUSE

O FUSE depende de plug-ins. A tabela a seguir lista os plug-ins comuns.

TABELA 19.1 PLUG-INS DISPONÍVEIS DO FUSE

`fuseiso`	monta imagens de CD-ROM contendo sistemas de arquivos ISO9660
`ntfs-3g`	monta volumes NTFS (com suporte de leitura e gravação)
`sshfs`	cliente de sistema de arquivos com base no protocolo de transferência de arquivo SSH
`wdfs`	monta sistemas de arquivos WebDAV

19.3 Para obter mais informações

Consulte a home page http://fuse.sourceforge.net do FUSE para obter mais informações.

III Serviços

20 Rede básica 250

21 Sincronização de horário com NTP 308

22 Usando o NetworkManager 315

23 Samba 325

24 Compartilhando sistemas de arquivos com o NFS 340

25 Montagem sob demanda com o Autofs 346

26 Sincronização de arquivos 355

20 Rede básica

O Linux oferece os recursos e as ferramentas de rede necessários para a integração em todos os tipos de estruturas de rede. É possível configurar o acesso a rede usando uma placa de rede com o YaST. A configuração também pode ser feita manualmente. Neste capítulo são abordados apenas os mecanismos fundamentais e os arquivos de configuração de rede relevantes.

Linux e outros sistemas operacionais Unix usam o protocolo TCP/IP. Não é um protocolo de rede único, mas uma família de protocolos de rede que oferece vários serviços. Os protocolos listados na *Vários protocolos na família de protocolos TCP/IP* são fornecidos com a finalidade de trocar dados entre duas máquinas por meio do TCP/IP. As redes combinadas por TCP/IP compõem uma rede mundial também chamada de "Internet".

RFC significa *Request for Comments*. Os RFCs são documentos que descrevem vários procedimentos de implementação e protocolos da Internet para o sistema operacional e seus aplicativos. Os documentos RFC descrevem a configuração dos protocolos da Internet. Para obter mais informações sobre RFCs, visite http://www.ietf.org/rfc.html.

VÁRIOS PROTOCOLOS NA FAMÍLIA DE PROTOCOLOS TCP/IP

TCP

Transmission Control Protocol: um protocolo seguro orientado por conexão. Os dados a serem transmitidos são enviados primeiramente pelo aplicativo como fluxo de dados e convertidos no formato adequado ao sistema operacional. Os dados chegam ao respectivo aplicativo no host de destino com o formato original de fluxo de dados no qual foram inicialmente enviados. O TCP determina se algum dado foi perdido ou embaralhado durante a transmissão. O TCP é implementado onde a sequência de dados for necessária.

UDP

User Datagram Protocol: um protocolo inseguro, não baseado em conexão. Os dados a serem transmitidos são enviados na forma de pacotes gerados pelo aplicativo. A ordem em que os dados chegam ao destinatário não é garantida, havendo possibilidade de perda dos dados. O UDP é adequado para aplicativos orientados por registro. Ele possui um período de latência menor que o TCP.

ICMP

Internet Control Message Protocol: essencialmente, não se trata de um protocolo para o usuário final, mas um protocolo de controle especial que emite relatórios de erros e pode controlar o comportamento de máquinas que participam da transferência de dados TCP/IP. Além disso, ele fornece um modo de eco especial, que pode ser visualizado usando o programa ping.

IGMP

Internet Group Management Protocol: esse protocolo controla o comportamento da máquina na implementação de multicast IP.

Conforme mostrado na *Figura 20.1, "Modelo de camadas simplificado para TCP/IP"*, a troca de dados ocorre em camadas diferentes. A camada de rede real é a transferência de dados insegura por IP (Internet protocol). Acima do IP, o TCP garante, até certo ponto, a segurança na transferência de dados. A camada IP é suportada pelo protocolo base dependente do hardware, como a Ethernet.

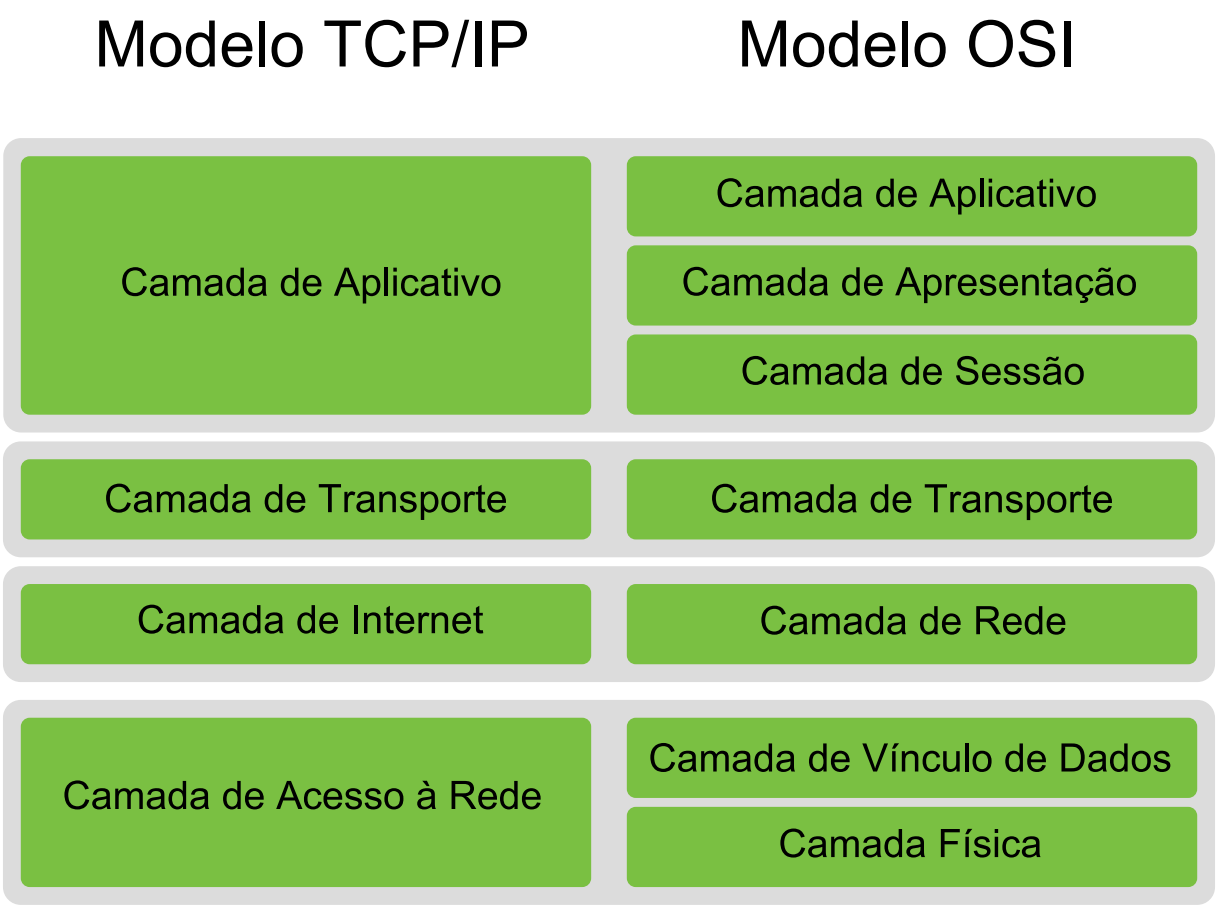


FIGURA 20.1 MODELO DE CAMADAS SIMPLIFICADO PARA TCP/IP

O diagrama fornece um ou dois exemplos para cada camada. As camadas são organizadas de acordo com os *níveis de abstração*. A camada mais baixa fica muito próxima do hardware. A camada mais alta é quase completamente abstraída do hardware. Todas as camadas possuem suas funções especiais próprias. As funções especiais de cada camada, na maioria das vezes, estão implícitas em suas descrições. A vinculação de dados e as camadas físicas representam a rede física usada, como a Ethernet.

Quase todos os protocolos de hardware funcionam em uma base orientada por pacotes. Os dados a serem transmitidos são reunidos em *pacotes* (não podem ser enviados todos de uma vez). O tamanho máximo de um pacote TCP/IP é de aproximadamente 64 KB. Os pacotes são normalmente bem menores, já que o hardware da rede pode ser um fator de limitação. O tamanho máximo de um pacote de dados na Ethernet é de cerca de 1.500 bytes. O tamanho do pacote TCP/IP limita-se a esse valor quando os dados são enviados por Ethernet. Se mais dados forem transferidos, mais pacotes de dados precisarão ser enviados pelo sistema operacional.

Para que as camadas executem suas respectivas funções, informações adicionais referentes a cada uma delas devem ser gravadas no pacote de dados. Isso ocorre no *cabeçalho* do pacote. Todas as camadas anexam um pequeno bloco de dados, chamado cabeçalho do protocolo, à frente de cada pacote emergente. Veja uma demonstração de pacote de dados TCP/IP passando por um cabo Ethernet na *Figura 20.2, "Pacote Ethernet TCP/IP"*. A soma de teste está localizada no final do pacote e não no início. Isso torna as coisas mais simples para o hardware de rede.

Cabeçalho Ethernet (14 bytes)
Cabeçalho IP (20 bytes)
Cabeçalho TCP (20 bytes)
Dados de Uso (máximo de 1460 bytes)
Checksum (2 bytes)

FIGURA 20.2 PACOTE ETHERNET TCP/IP

Quando um aplicativo envia dados pela rede, os dados passam por cada camada, todas implementadas no Kernel do Linux, exceto a camada física. Cada camada é responsável pela preparação dos dados, para que eles possam passar para a camada seguinte. A camada mais baixa é a responsável pelo envio de dados. Todo o processo é invertido quando os dados são recebidos. Como camadas de uma cebola, em cada uma os cabeçalhos de protocolo são removidos dos dados transportados. Por fim, a camada de transporte é responsável por disponibilizar os dados para uso pelos aplicativos de destino. Dessa forma, cada camada se comunica somente com a camada diretamente acima ou abaixo dela. Para os aplicativos, é irrelevante se os dados são transmitidos por rede FDDI de 100 Mbits/s ou por linha de modem de 56 Kbits/s. Da mesma forma, é irrelevante para a linha de dados os tipos de dados transmitidos, contanto que os pacotes estejam no formato correto.

20.1 Roteamento e endereços IP

Esta seção limita-se à abordagem de redes IPv4. Para obter informações sobre o protocolo IPv6, sucessor do IPv4, consulte a *Seção 20.2, "IPv6 — A Internet da próxima geração"*.

20.1.1 Endereços IP

Todo computador na Internet possui um endereço de 32 bits exclusivo. Os 32 bits (ou 4 bytes) normalmente são gravados conforme ilustrado na segunda linha em *Exemplo 20.1, "Gravando endereços IP"*.

EXEMPLO 20.1 GRAVANDO ENDEREÇOS IP

```
IP Address (binary):  11000000 10101000 00000000 00010100
IP Address (decimal):      192.     168.       0.      20
```

Na forma decimal, os quatro bytes são gravados no sistema de números decimais, separados por pontos. O endereço IP é designado a um host ou a uma interface de rede. Ele pode ser usado apenas uma vez em todo o mundo. Há exceções a essa regra, mas não são relevantes para as passagens a seguir.

Os pontos nos endereços IP indicam o sistema hierárquico. Até os anos 90, os endereços IP eram estritamente categorizados em classes. Entretanto, esse sistema demonstrou ser excessivamente inflexível e foi desativado. Agora, o *CIDR* (Classless Interdomain Routing — Roteamento Interdomínio sem Classes) é usado.

20.1.2 Máscaras de rede e roteamento

As máscaras de rede são usadas para definir a faixa de endereços de uma sub-rede. Se dois hosts estiverem na mesma sub-rede, eles poderão acessar um ao outro diretamente. Se não estiverem na mesma sub-rede, eles precisarão do endereço de um gateway que manipule todo o tráfego da sub-rede. Para verificar se dois endereços IP estão em uma mesma sub-rede, basta "E" os dois endereços com a máscara de rede. Se o resultado for idêntico, os dois endereços IP estarão na mesma rede local. Se houver diferenças, o endereço IP remoto e, portanto, a interface remota, só poderão ser localizados através de um gateway.

Para compreender como as máscaras de rede funcionam, consulte o *Exemplo 20.2, "Vinculando endereços IP à máscara de rede"*. A máscara de rede consiste em 32 bits que identificam o quanto um endereço IP pertence à rede. Todos os bits `1` marcam o bit correspondente no endereço IP como pertencente à rede. Todos os bits `0` marcam os bits dentro da sub-rede. Isso significa que quanto maior a quantidade de bits `1`, menor será o tamanho da sub-rede. Como a máscara de rede sempre consiste em vários bits `1` sucessivos, também é possível contar o número de bits da máscara de rede. Na *Exemplo 20.2, "Vinculando endereços IP à máscara de rede"*, a primeira rede com 24 bits também pode ser gravada como `192.168.0.0/24`.

EXEMPLO 20.2 VINCULANDO ENDEREÇOS IP À MÁSCARA DE REDE

```
IP address (192.168.0.20):  11000000 10101000 00000000 00010100
Netmask   (255.255.255.0):  11111111 11111111 11111111 00000000
------------------------------------------------------------
Result of the link:         11000000 10101000 00000000 00000000
In the decimal system:           192.     168.       0.       0

IP address (213.95.15.200): 11010101 10111111 00001111 11001000
Netmask    (255.255.255.0): 11111111 11111111 11111111 00000000
------------------------------------------------------------
Result of the link:         11010101 10111111 00001111 00000000
In the decimal system:           213.      95.      15.       0
```

Para dar outro exemplo: todas as máquinas conectadas ao mesmo cabo Ethernet, normalmente, estão localizadas na mesma sub-rede e são diretamente acessíveis. Mesmo quando a sub-rede é dividida fisicamente por switches ou pontes, esses hosts ainda assim podem ser diretamente localizados.

Endereços IP fora da sub-rede local só poderão ser localizados se um gateway for configurado para a rede de destino. Nos casos mais comuns, há somente um gateway que controla todo o tráfego externo. Entretanto, também é possível configurar vários gateways para sub-redes diferentes.

Se um gateway tiver sido configurado, todos os pacotes IP externos serão enviados para o gateway apropriado. Esse gateway tentará então encaminhar os pacotes da mesma forma (de host para host) até acessar o host de destino ou até o TTL (time to live) do pacote expirar.

ENDEREÇOS ESPECÍFICOS

Endereço de rede base

Essa é a máscara de rede E qualquer endereço na rede, conforme mostrado no *Exemplo 20.2, "Vinculando endereços IP à máscara de rede"* em `Resultado`. Esse endereço não pode ser designado a nenhum host.

Endereço de broadcast

Isso pode ser parafraseado como: "Acessar todos os hosts nesta sub-rede." Para gerar isso, a máscara de rede é invertida no formato binário e vinculada ao endereço de rede base com um OU lógico. Portanto, o exemplo acima resulta em 192.168.0.255. Esse endereço não pode ser atribuído a nenhum host.

Host local

O endereço `127.0.0.1` é designado ao "dispositivo loopback" em cada host. Pode-se configurar uma conexão para a sua própria máquina com este endereço e com todos os endereços da rede de loopback completa `127.0.0.0/8`, conforme definidos com o IPv4. Com o IPv6, existe apenas um endereço de loopback (`::1`).

Como os endereços IP precisam ser exclusivos em qualquer parte do mundo, não é possível selecionar endereços aleatoriamente. Há três domínios de endereços a serem usados para configurar uma rede baseada em IP privado. Eles não conseguem se conectar ao restante da Internet, pois não podem ser transmitidos através dela. Esses domínios de endereço são especificados no RFC 1597 e listados na *Tabela 20.1, "Domínios de endereços IP privados"*.

TABELA 20.1 DOMÍNIOS DE ENDEREÇOS IP PRIVADOS

Rede/máscara de rede	Domínio
`10.0.0.0`/`255.0.0.0`	`10.x.x.x`
`172.16.0.0`/`255.240.0.0`	`172.16.x.x` – `172.31.x.x`
`192.168.0.0`/`255.255.0.0`	`192.168.x.x`

20.2 IPv6 — A Internet da próxima geração

Devido ao surgimento da WWW (World Wide Web), a Internet teve um crescimento acelerado com um número cada vez maior de computadores se comunicando por TCP/IP nos últimos 15 anos. Desde que Tim Berners-Lee da CERN (http://public.web.cern.ch) inventou a WWW em 1990, o número de hosts da Internet cresceu de poucos milhares para centenas de milhões deles.

Conforme mencionado, um endereço IPv4 consiste em apenas 32 bits. Além disso, muitos endereços IP são perdidos, eles não podem ser usados devido à forma como as redes são organizadas. O número de endereços disponíveis na sua sub-rede é dois elevado à potência do número de bits, menos dois. Uma sub-rede tem, por exemplo, 2, 6 ou 14 endereços disponíveis. Para conectar 128 hosts à Internet, por exemplo, você precisa de uma sub-rede com 256 endereços IP, dos quais apenas 254 são utilizáveis, visto que são necessários dois endereços IP para a estrutura da própria sub-rede: o endereço de broadcast e o endereço de rede base.

No protocolo IPv4 atual, DHCP ou NAT (Network Address Translation — Conversão de Endereços de Rede) são os mecanismos comuns usados para contornar a grande falta de endereços. Combinado à convenção de manter endereços públicos e privados separados por espaços, esses métodos podem certamente reduzir a falta de endereços. O problema deles está em suas configurações, trabalhosas para configurar e difíceis de manter. Para configurar um host em uma rede IPv4, é preciso que haja vários itens de endereços, como o próprio endereço IP do host, a máscara de sub-rede, o endereço de gateway e talvez um endereço de servidor de nomes. Todos esses itens precisam ser conhecidos e não podem ser derivados de outro lugar.

Com o IPv6, tanto a falta de endereços quanto as configurações complicadas passariam a ser problemas do passado. As seções a seguir oferecem mais informações sobre os aprimoramentos e benefícios trazidos pelo IPv6 e sobre a transição do protocolo antigo para o novo.

20.2.1 Vantagens

A melhoria mais importante e visível oferecida pelo novo protocolo é a expansão enorme do espaço disponível para endereços. Um endereço IPv6 é composto por valores de 128 bits, em vez dos 32 bits tradicionais. Ele é capaz de fornecer 'quatrilhões' de endereços IP.

Entretanto, os endereços IPv6 não diferem de seus antecessores apenas em relação ao comprimento. Também possuem uma estrutura interna diferente, que pode conter mais informações específicas sobre os sistemas e as redes a que pertencem. Leia mais detalhes sobre eles na *Seção 20.2.2, “Estrutura e tipos de endereços”*.

A seguir, há uma lista de algumas outras vantagens do novo protocolo:

Configuração automática

O IPv6 torna apto o “plug and play” da rede, o que significa que um sistema recentemente configurado é integrado à rede (local) sem qualquer configuração manual. O novo host usa seu mecanismo de configuração automática para derivar seu próprio endereço a partir das informações disponibilizadas pelos roteadores vizinhos, com base em um protocolo chamado *ND* (Neighbor Discovery — descoberta de vizinho). Esse método não exige nenhuma intervenção por parte do administrador e não há necessidade de manter um servidor central para alocação de endereços; uma vantagem adicional em relação ao IPv4, cuja alocação automática de endereços exige um servidor DHCP.

No entanto, se houver um roteador conectado a um switch, ele deverá enviar anúncios periódicos com flags avisando os hosts de uma rede como eles devem interagir entre si. Para obter mais informações, consulte o RFC 2462 e a página de manual de `radvd.conf(5)`, e o RFC 3315.

Mobilidade

O IPv6 torna possível a atribuição de vários endereços a uma interface de rede ao mesmo tempo. Isso permite que os usuários acessem várias redes com facilidade, algo comparável aos serviços de roaming internacional oferecidos por operadoras de telefonia celular: quando você leva seu telefone celular para o exterior, ele se registra automaticamente em um serviço estrangeiro logo que entra na área correspondente, de modo que você possa ser contatado pelo mesmo número em qualquer lugar e ligar para alguém como se estivesse em sua área de origem.

Comunicação segura

Com o IPv4, a segurança da rede é uma função adicional. O IPv6 inclui IPsec como um de seus recursos principais, permitindo que sistemas se comuniquem por um túnel seguro, para evitar a intromissão de estranhos na Internet.

Compatibilidade retroativa

De forma realista, seria impossível mudar toda a Internet de IPv4 para IPv6 de uma só vez. Portanto, é essencial que ambos os protocolos sejam capazes de coexistir na Internet, mas também em um sistema. Isso é garantido por endereços compatíveis (endereços IPv4 podem facilmente ser convertidos em endereços IPv6) e através do uso de vários túneis. Consulte a *Seção 20.2.3, “Coexistência de IPv4 e IPv6”*. Da mesma forma, os sistemas podem se basear em uma técnica *IP de pilha dupla* para suportar os dois protocolos ao mesmo tempo, significando que possuem duas pilhas de rede completamente separadas, de tal forma que não há interferência entre as duas versões de protocolos.

Serviços adaptados e personalizados através de Multicast

Com o IPv4, alguns serviços, como SMB, precisam transmitir seus pacotes para todos os host na rede local. O IPv6 oferece uma abordagem mais detalhada, permitindo que os servidores enviem hosts através de *multicast* — determinando um número de hosts como partes de um grupo (o que é diferente de direcionar todos os hosts através de *broadcast* ou cada host individualmente através de *unicast*). Os hosts enviados como grupos talvez dependam do aplicativo concreto. É possível enviar todos os servidores de nomes para alguns grupos predefinidos (o *grupo multicast de servidores de nomes*), por exemplo ou todos os roteadores (o *grupo multicast de todos os roteadores*).

20.2.2 Estrutura e tipos de endereços

Conforme mencionado, o protocolo IP atual está em desvantagem em relação a dois aspectos importantes: os endereços IP estão cada vez mais escassos, e a configuração de rede com manutenção de tabelas de rotina vem se tornando cada vez mais uma tarefa complexa e onerosa. O IPv6 soluciona o primeiro problema expandindo o espaço dos endereços para 128 bits. O segundo problema é contornado com a introdução de uma estrutura hierárquica de endereços, combinada com técnicas sofisticadas para alocar endereços de rede, assim como *multihoming* (a capacidade de designar vários endereços a um dispositivo, permitindo acesso a diversas redes).

Ao utilizar o IPv6, é útil saber que há três tipos diferentes de endereços:

Unicast

Endereços desse tipo são associados com exatamente uma interface de rede. Pacotes com esse tipo de endereço são entregues em apenas um destino. Da mesma forma, os endereços unicast são usados para transferir pacotes para hosts individuais na rede local ou na Internet.

Multicast

Endereços desse tipo estão relacionados a um grupo de interfaces de rede. Pacotes com esse tipo de endereço são entregues a todos os destinos pertencentes ao grupo. Endereços multicast são usados, principalmente, por certos tipos de serviços de rede para se comunicarem com determinados grupos de host de forma bem direcionada.

Anycast

Endereços desse tipo estão relacionados a um grupo de interfaces. Pacotes com esse tipo de endereço são entregues ao membro do grupo mais próximo do remetente, de acordo com os princípios do protocolo de roteamento subjacente. Endereços anycast são usados para que hosts possam descobrir mais facilmente servidores que oferecem certos serviços na área da rede determinada. Todos os servidores do mesmo tipo possuem o mesmo endereço anycast. Sempre que um host solicita um serviço, ele recebe uma resposta do servidor com o local mais próximo, conforme determinado pelo protocolo de roteamento. Caso ocorra alguma falha com esse servidor, o protocolo selecionará automaticamente o segundo servidor mais próximo ou então o terceiro e assim por diante.

Um endereço IPv6 é constituído de oito campos de quatro dígitos, cada um representando 16 bits, gravados em notação hexadecimal. Eles são separados por dois-pontos (`:`). Quaisquer zero bytes iniciais em um determinado campo podem ser descartados, mas zeros dentro ou no final do campo não podem ser descartados. Outra convenção é a de que mais de quatro zero bytes

consecutivos podem retornar como dois-pontos duplos. Entretanto, apenas um separador do tipo `::` é permitido por endereço. Esse tipo de notação reduzida é mostrado no *Exemplo 20.3, "Amostra de endereço IPv6"*, em que todas as três linhas representam o mesmo endereço.

EXEMPLO 20.3 AMOSTRA DE ENDEREÇO IPV6

```
fe80 : 0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4
fe80 :    0 :    0 :    0 :    0 : 10 : 1000 : 1a4
fe80 :                            : 10 : 1000 : 1a4
```

Cada parte de um endereço IPv6 possui uma função definida. Os primeiros bytes formam o prefixo e especificam o tipo de endereço. A parte central é a porção do endereço na rede, mas pode não ser utilizada. O final do endereço forma a parte do host. Com o IPv6, a máscara de rede é definida indicando o comprimento do prefixo depois de uma barra no final do endereço. Um endereço, como mostrado no *Exemplo 20.4, "Endereço IPv6 especificando o comprimento do prefixo"*, contém as informações de que os primeiros 64 bits formam a parte da rede do endereço e que os últimos 64 formam a parte do host. Em outras palavras, `64` significa que a máscara de rede está preenchida com 64 valores de 1 bit a partir da esquerda. Como no IPv4, o endereço IP é combinado com E, com os valores da máscara de rede, para determinar se o host está localizado na mesma sub-rede ou em outra.

EXEMPLO 20.4 ENDEREÇO IPV6 ESPECIFICANDO O COMPRIMENTO DO PREFIXO

```
fe80::10:1000:1a4/64
```

O IPv6 conhece vários tipos de prefixos predefinidos. Alguns são mostrados na *Vários prefixos IPv6*.

VÁRIOS PREFIXOS IPV6

`00`
: Endereços IPv4 e endereços de compatibilidade de IPv4 sobre IPv6. Esses são usados para manter a compatibilidade com IPv4. O seu uso ainda exige um roteador capaz de converter pacotes IPv6 em pacotes IPv4. Vários endereços especiais, como o do dispositivo loopback, também possuem esse prefixo.

`2` ou `3` como o primeiro dígito
: Endereços unicast globais agregativos. Como no caso do IPv4, uma interface pode ser atribuída para fazer parte de determinada sub-rede. Atualmente, existem os seguintes espaços de endereço: `2001::/16` (espaço de endereço de qualidade de produção) e `2002::/16` (espaço de endereço 6to4).

`fe80::/10`

Endereços locais de links. Endereços com este prefixo não devem ser roteados e, portanto, só devem ser encontrados na mesma sub-rede.

`fe80::/10`

Endereços locais de sites. Esses podem ser roteados, mas somente na rede da organização a que pertencem. Na verdade, eles são o equivalente IPv6 do espaço de endereço de rede privada atual, como `10.x.x.x`.

`ff`

Esses são endereços multicast.

Um endereço unicast consiste em três componentes básicos:

Topologia pública

A primeira parte (que também contém um dos prefixos mencionados acima) é usada para rotear pacotes através da Internet pública. Ela inclui informações sobre a empresa ou instituição que fornece o acesso à Internet.

Topologia do site

A segunda parte contém informações de roteamento sobre a sub-rede à qual o pacote deve ser entregue.

ID de interface

A terceira parte identifica a interface à qual o pacote deve ser entregue. Isso também permite que o MAC faça parte do endereço. Como MAC é um identificador fixo globalmente exclusivo codificado no dispositivo pelo fabricante do hardware, o procedimento de configuração é bastante simplificado. Na verdade, os primeiros 64 bits de endereço são consolidados para formar o token `EUI-64`, com os últimos 48 bits obtidos no MAC e os 24 bits restantes contendo informações especiais sobre o tipo de token. Isso também permite atribuir um token `EUI-64` a interfaces que não tenham MAC, como aquelas baseadas em PPP.

No topo dessa estrutura básica, o IPv6 faz distinção entre cinco tipos de endereços unicast:

`::` (não especificado)

Esse endereço é usado pelo host como seu endereço de origem durante a primeira inicialização da interface, quando o endereço ainda não pode ser determinado por outros meios.

`::1` (loopback)

O endereço do dispositivo loopback.

Endereços compatíveis com o IPv4

O endereço IPv6 é formado pelo endereço IPv4 e um prefixo consistindo em 96 zero bits. Esse tipo de endereço de compatibilidade é usado para um túnel (consulte a *Seção 20.2.3, "Coexistência de IPv4 e IPv6"*) para permitir que os hosts IPv4 e IPv6 se comuniquem com outros que estejam operando em um ambiente IPv4 puro.

Endereços IPv4 mapeados para IPv6

Esse tipo de endereço especifica um endereço IPv4 puro em uma notação IPv6.

Endereços locais

Há dois tipos de endereços para uso local:

link-local

Este tipo de endereço só pode ser usado na sub-rede local. Pacotes com endereço de origem ou de destino desse tipo não devem ser roteados para a Internet nem para outras sub-redes. Esses endereços contêm um prefixo especial (`fe80::/10`) e o ID da interface da placa de rede, com a parte do meio consistindo em zero bytes. Endereços desse tipo são usados durante a configuração automática para se comunicarem com outros hosts pertencentes à mesma sub-rede.

site-local

Pacotes com este tipo de endereço podem ser roteados para outras sub-redes, mas não para a Internet mais ampla. Eles devem permanecer dentro da própria rede da organização. Tais endereços são usados para intranets e equivalem ao espaço de endereço privado definido pelo IPv4. Eles contêm um prefixo especial (`fec0::/10`), o ID da interface e um campo de 16 bits que especifica o ID da sub-rede. Novamente, o restante é preenchido com bytes zero.

Como um recurso completamente novo, introduzido com o IPv6, cada interface de rede normalmente obtém vários endereços IP, com a vantagem de que várias redes podem ser acessadas através da mesma interface. Uma dessas redes pode ser totalmente configurada automaticamente usando o MAC e um prefixo conhecido, resultando na possibilidade de todos os hosts na rede local serem encontrados assim que o IPv6 for habilitado (usando o endereço link-local). Com o MAC fazendo parte disso, qualquer endereço IP usado no mundo será exclusivo. As únicas partes variáveis do endereço são aquelas que indicam a *topologia do site* e a *topologia pública*, dependendo da rede real na qual o host estiver operando no momento.

Para que um host avance e retroceda entre duas redes diferentes ele precisa de, pelo menos, dois endereços. Um deles, o *endereço pessoal*, contém não só o ID de interface, como também um identificador da rede doméstica a que ele normalmente pertence (e o prefixo correspondente). O endereço pessoal é um endereço estático e, portanto, normalmente não se modifica. Mesmo assim, todos os pacotes destinados ao host móvel podem ser entregues a ele, independentemente de ele operar na rede doméstica ou em outro local externo. Isso é possível devido aos recursos totalmente novos introduzidos com o IPv6, como *configuração automática sem estado* e *descoberta de vizinho*. Além do endereço residencial, um host móvel obtém um ou mais endereços adicionais pertencentes às redes interurbanas com roaming. Eles são chamados endereços *care-of*. A rede doméstica tem um recurso que encaminha qualquer pacote destinado ao host quando ele está em roaming. Em um ambiente IPv6, essa tarefa é executada pelo *agente local*, que retransmite todos os pacotes destinados ao endereço residencial através de um túnel. Por outro lado, esses pacotes destinados ao endereço care-of são diretamente transferidos para o host móvel sem qualquer desvio especial.

20.2.3 Coexistência de IPv4 e IPv6

A migração de todos os hosts conectados à Internet do IPv4 para o IPv6 é um processo gradual. Os dois protocolos coexistirão durante algum tempo. A coexistência deles em um sistema é garantida onde houver uma implementação de *pilha dupla* de ambos os protocolos. Ainda resta a dúvida de como um host habilitado do IPv6 deve se comunicar com um host IPv4 e como pacotes do IPv6 devem ser transportados pelas redes atuais, que são predominantemente baseadas no IPv4. As melhores soluções oferecem endereços de compatibilidade e túnel (consulte a *Seção 20.2.2, “Estrutura e tipos de endereços”*).

Os hosts IPv6 que estiverem mais ou menos isolados na rede IPv4 (mundial) podem se comunicar por túneis: os pacotes IPv6 são encapsulados como pacotes IPv4 para que sejam transmitidos por uma rede IPv4. Tal conexão entre dois hosts IPv4 é chamada de *túnel*. Para que isso ocorra, os pacotes precisam incluir o endereço de destino do IPv6 (ou o prefixo correspondente), assim como o endereço IPv4 do host remoto no destino final do túnel. Um túnel básico pode ser configurado manualmente, de acordo com um contrato entre os administradores dos hosts. Também é chamado de *túnel estático*.

Entretanto, a configuração e manutenção de túneis estáticos é normalmente muito trabalhosa para ser usada diariamente em comunicações. Portanto, o IPv6 fornece três métodos de *túneis dinâmicos*:

6over4

Os pacotes IPv6 são automaticamente encapsulados como pacotes IPv4 e enviados por uma rede IPv4 com capacidade multicast. O IPv6 é induzido a considerar a rede inteira (Internet) como uma gigantesca rede local. Com isso, é possível determinar automaticamente o destino final do túnel IPv4. Entretanto, esse método não faz um dimensionamento muito bom e também é dificultado pelo fato de o multicast IP não ser tão difundido na Internet. Portanto, ele apenas fornece uma solução para redes corporativas ou institucionais menores, em que o multicast pode ser habilitado. As especificações para esse método estão descritas no RFC 2529.

6to4

Com esse método, os endereços IPv4 são automaticamente gerados a partir de endereços IPv6, habilitando a comunicação de hosts IPv6 isolados através de uma rede IPv4. Entretanto, alguns problemas foram relatados no que tange à comunicação entre esses hosts IPv6 isolados e a Internet. O método está descrito no RFC 3056.

Controlador do túnel IPv6

Esse método se baseia em servidores especiais que fornecem túneis dedicados para hosts IPv6. É descrito no RFC 3053.

20.2.4 Configurando o IPv6

Para configurar o IPv6, normalmente não é necessário fazer mudanças nas estações de trabalho individuais. O IPv6 é habilitado por padrão. Para desabilitar ou habilitar o IPv6 em um sistema instalado, use o módulo *Configurações de Rede* do YaST. Na guia *Opções Globais*, marque ou desmarque a opção *Habilitar IPv6* conforme for necessário. Para habilitá-lo temporariamente até a próxima reinicialização, digite `modprobe -i ipv6` como `root`. É impossível descarregar o módulo IPv6 depois de carregado.

Devido ao conceito de configuração automática do IPv6, um endereço é designado à placa de rede na rede *link-local*. Normalmente, nenhum gerenciamento de tabela de roteamento é feito em uma estação de trabalho. Os roteadores de rede podem ser consultados pela estação de trabalho, usando o *protocolo de anúncios do roteador*, para o qual devem ser implementados um prefixo e gateways. O programa radvd pode ser usado para configurar um roteador IPv6.

Esse programa informa às estações de trabalho o prefixo que deve ser usado para os endereços IPv6 e os roteadores. Outra opção é usar zebra/quagga para a configuração automática dos dois endereços e para roteamento.

Para obter informações sobre como configurar vários tipos de túneis usando os arquivos `/etc/sysconfig/network`, consulte a página de manual de `ifcfg-tunnel` (**`man ifcfg-tunnel`**).

20.2.5 Para obter mais informações

A visão geral acima não abrange totalmente o tópico do IPv6. Para obter informações mais detalhadas sobre o novo protocolo, consulte os livros e a documentação online a seguir:

http://www.ipv6.org/

O ponto de partida para tudo relativo ao IPv6.

http://www.ipv6day.org

Todas as informações necessárias para iniciar sua própria rede IPv6.

http://www.ipv6-to-standard.org/

A lista de produtos habilitados para IPv6.

http://www.bieringer.de/linux/IPv6/

Aqui, encontre o Linux IPv6-HOWTO e muitos links relacionados ao tópico.

RFC 2640

Informações fundamentais do RFC sobre o IPv6.

IPv6 Essentials

Um livro que descreve todos os aspectos importantes do tópico é o *IPv6 Essentials* de Silvia Hagen (ISBN 0-596-00125-8).

20.3 Resolução de nomes

O DNS ajuda na designação de um endereço IP a um ou mais nomes e na designação de um nome a um endereço IP. No Linux, essa conversão normalmente é executada por um tipo especial de software chamado bind. A máquina responsável por essa conversão é chamada de *servidor de nomes*. Os nomes criam um sistema hierárquico, no qual cada componente do nome é separado um ponto. A hierarquia de nomes é, entretanto, independente da hierarquia de endereços IP descrita acima.

Considere um nome completo, como `jupiter.exemplo.com`, escrito no formato `nome_de_host.domínio`. Um nome completo, denominado *FQDN* (Fully Qualified Domain Name – Nome de Domínio Completo e Qualificado), consiste em um nome de host e um nome de domínio (`exemplo.com`). O último também inclui o *TLD* (Top Level Domain — Domínio de Nível Superior) (`com`).

A designação TLD tornou-se bastante confusa por razões históricas. Tradicionalmente, nomes de domínio com três letras são usados nos EUA. No resto do mundo, os códigos nacionais ISO de duas letras são o padrão. Além disso, TLDs mais longos foram introduzidos em 2000, representando certas esferas de atividades (por exemplo, `.info`, `.name`, `.museum`).

No início da Internet (antes de 1990), o arquivo `/etc/hosts` era usado para armazenar os nomes de todas as máquinas representadas na Internet. Isso rapidamente se tornou impraticável, devido ao crescente número de computadores conectados à Internet. Por essa razão, um banco de dados descentralizado foi desenvolvido para armazenar nomes de host de uma forma amplamente distribuída. Esse banco de dados, semelhante ao servidor de nomes, não possui os dados pertencentes a todos os hosts na Internet já disponíveis, mas pode encaminhar solicitações a outros servidores de nomes.

A parte superior da hierarquia é ocupada pelos *servidores de nomes raiz*. Esses servidores de nomes raiz gerenciam os domínios de nível superior e são executados pelo NIC (Network Information Center). Cada servidor de nomes raiz conhece os servidores de nomes responsáveis por um determinado domínio de nível superior. Para obter informações sobre NICs de domínio superior, vá para http://www.internic.net.

O DNS pode fazer mais do que resolver nomes de host. O servidor de nomes também distingue qual host recebe e-mails para um domínio inteiro: o *MX (servidor de correio)*.

Para sua máquina resolver um endereço IP, ela precisa pelo menos conhecer um servidor de nomes e seu respectivo endereço IP. É fácil especificar esse servidor de nomes com a ajuda do YaST. Se você tiver uma conexão de discagem por modem, talvez não precise nem mesmo configurar um servidor de nomes manualmente. O protocolo de discagem fornece o endereço do servidor de nomes enquanto a conexão é efetuada.

O protocolo `whois` está intimamente relacionado ao DNS. Com esse programa, é possível descobrir rapidamente o responsável por qualquer domínio especificado.

Nota: MDNS e nomes do domínio .local

O domínio de nível superior `.local` é tratado como domínio link-local pelo resolver. As solicitações de DNS são enviadas como solicitações de DNS multicast, em vez de solicitações de DNS normal. Se você já usa o domínio `.local` em sua configuração de servidor de nomes, deverá desativar essa opção em `/etc/host.conf`. Para obter mais informações, consulte a página de manual `host.conf`.

Se desejar desativar o MDNS durante a instalação, use `nomdns=1` como parâmetro de boot.

Para obter mais informações sobre DNS de multicast, consulte http://www.multicastdns.org.

20.4 Configurando uma conexão de rede com o YaST

Há muitos tipos de redes suportadas no Linux. A maioria delas usa nomes de dispositivos diferentes e os arquivos de configuração se espalham por vários locais no sistema de arquivos. Para obter uma visão geral detalhada dos aspectos da configuração manual de rede, consulte a *Seção 20.6, "Configurando uma conexão de rede manualmente"*.

No SUSE Linux Enterprise Desktop, em que o NetworkManager está ativo por padrão, todas as placas de rede estão configuradas. Se o NetworkManager não estiver ativo, apenas a primeira interface com link ativo (com cabo de rede conectado) será configurada automaticamente. Hardwares adicionais podem ser configurados a qualquer momento no sistema instalado. As seguintes seções descrevem a configuração de rede para todos os tipos de conexões de rede suportadas pelo SUSE Linux Enterprise Desktop.

20.4.1 Configurando a placa de rede com o YaST

Para configurar a placa Ethernet ou Wi-Fi/Bluetooth no YaST, selecione *Dispositivos de Rede* › *Configurações de Rede*. Após iniciar o módulo, o YaST exibirá a caixa de diálogo *Configurações de Rede* com quatro guias: *Opções Globais*, *Visão Geral*, *Nome de host/DNS* e *Roteamento*.

A guia *Opções Globais* permite definir opções gerais de rede, como método de configuração de rede, IPv6 e opções gerais de DHCP. Para obter mais informações, consulte a *Seção 20.4.1.1, "Configurando opções globais de rede"*.

A guia *Visão Geral* contém informações sobre interfaces de rede instaladas e configurações. Ela lista os nomes de todas as placas de rede detectadas corretamente. Nessa caixa de diálogo, você pode configurar manualmente novas placas, bem como remover ou mudar suas configurações. Se você quiser configurar manualmente uma placa que não foi detectada automaticamente, consulte a *Seção 20.4.1.3, "Configurando uma placa de rede não detectada"*. Se você quiser mudar a configuração de uma placa que já está configurada, consulte a *Seção 20.4.1.2, "Mudando a configuração de uma placa de rede"*.

A guia *Nome de host/DNS* permite definir o nome de host da máquina e nomear os servidores que serão usados. Para obter mais informações, consulte a *Seção 20.4.1.4, "Configurando nome de host e DNS"*.

A guia *Roteamento* é usada para a configuração do roteamento. Consulte a *Seção 20.4.1.5, "Configurando o roteamento"* para obter mais informações.

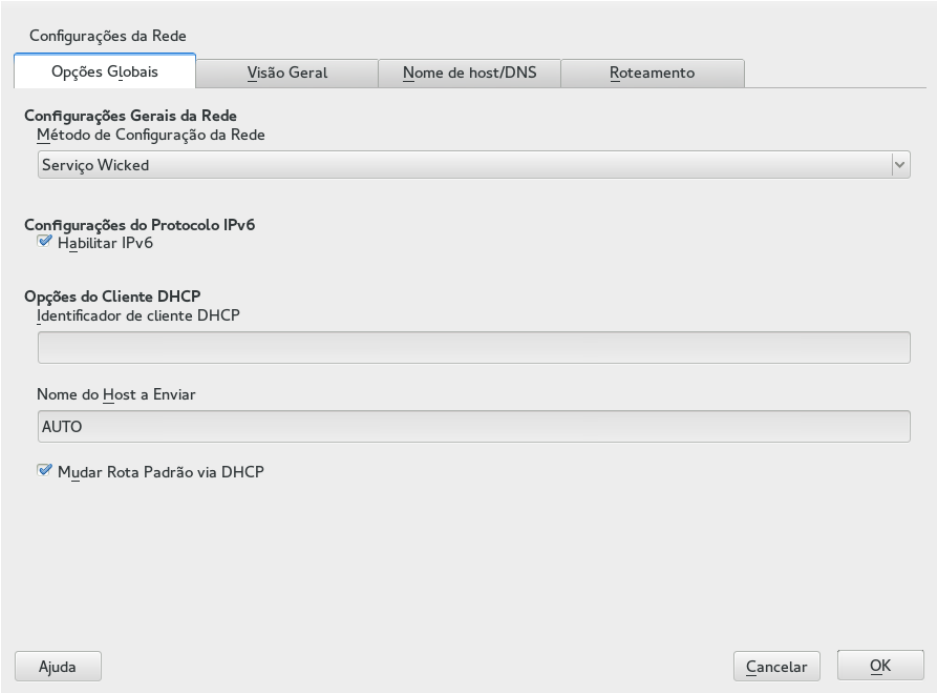


FIGURA 20.3 DEFININDO AS CONFIGURAÇÕES DA REDE

20.4.1.1 Configurando opções globais de rede

A guia *Opções Globais* do módulo *Configurações de Rede* do YaST permite definir opções globais de rede importantes, como o uso do NetworkManager, o IPv6 e opções de cliente DHCP. Essas configurações são aplicáveis a todas as interfaces de rede.

Em *Método de Configuração da Rede*, escolha o modo como as conexões de rede são gerenciadas. Para que um applet de área de trabalho do NetworkManager gerencie as conexões de todas as interfaces, escolha *Serviço do NetworkManager*. O NetworkManager é ideal para alternar entre várias redes com fio e wireless. Se você não tem um ambiente de área de trabalho em execução, ou se o seu computador for um servidor Xen, um sistema virtual ou fornecer serviços de rede como DHCP ou DNS em sua rede, use o método *Serviço Wicked*. Se o NetworkManager for usado, o **`nm-applet`** deverá ser usado para configurar opções de rede, e as guias *Visão Geral*, *Nome de host/DNS* e *Roteamento* do módulo *Configurações de Rede* estarão desabilitadas. Para obter mais informações sobre o NetworkManager, consulte o *Capítulo 22, Usando o NetworkManager*.

Em *Configurações do Protocolo IPv6*, escolha se é para usar o protocolo IPv6. É possível usar o IPv6 juntamente com o IPv4. Por padrão, IPv6 está habilitado. Contudo, nas redes que não usam o protocolo IPv6, os tempos de resposta podem ser acelerados com o protocolo IPv6 desabilitado. Para desabilitá-lo, desmarque *Habilitar IPv6*. Se o IPv6 for desabilitado, o Kernel não carregará mais o módulo IPv6 automaticamente. Esta configuração será aplicada após a reinicialização.

Nas *Opções do Cliente DHCP*, configure as opções do cliente DHCP. O *Identificador de Cliente DHCP* deve ser diferente para cada cliente DHCP na mesma rede. Se ficar vazio, assumirá como padrão o endereço de hardware da interface da rede. Entretanto, se você tiver várias máquinas virtuais em execução na mesma interface de rede e, portanto, com o mesmo endereço de hardware, especifique aqui um identificador exclusivo.

O *Nome do Host a Enviar* especifica uma string usada no campo da opção de nome de host quando o cliente DHCP envia mensagens ao servidor DHCP. Alguns servidores DHCP atualizam as zonas do servidor de nomes (registros diretos e reversos) de acordo com esse nome de host (DNS Dinâmico). Além disso, alguns servidores DHCP exigem que o campo da opção *Nome do Host a Enviar* contenha uma string específica nas mensagens DHCP dos clientes. Mantenha `AUTO` para enviar o nome de host atual (ou seja, o que está definido em `/etc/HOSTNAME`). Deixe o campo da opção vazio para não enviar nenhum nome de host.

Para não mudar a rota padrão de acordo com as informações do DHCP, desmarque *Mudar Rota Padrão via DHCP*.

20.4.1.2 Mudando a configuração de uma placa de rede

Para mudar a configuração de uma placa de rede, selecione-a na lista de placas detectadas em *Configurações de Rede* › *Visão Geral* no YaST e clique em *Editar*. A caixa de diálogo *Configuração da Placa de Rede* é exibida, na qual é possível ajustar a configuração da placa usando as guias *Geral*, *Endereço* e *Hardware*.

20.4.1.2.1 Configurando endereços IP

Você pode definir o endereço IP da placa de rede ou o modo como seu endereço IP é determinado na guia *Endereço* da caixa de diálogo *Configuração da Placa de Rede*. Há suporte para endereços IPv4 e IPv6. A placa de rede pode ser *Sem Endereço IP* (útil para dispositivos de vinculação), ter um *Endereço IP Atribuído Estaticamente* (IPv4 ou IPv6) ou um *Endereço Dinâmico* atribuído por *DHCP*, *Zeroconf* ou ambos.

Ao usar um *Endereço Dinâmico*, selecione se deseja usar *Apenas DHCP Versão 4* (para IPv4), *Apenas DHCP Versão 6* (para IPv6) ou *DHCP Versões 4 e 6*.

Se possível, a primeira placa de rede com link que estiver disponível durante a instalação será configurada automaticamente para usar a configuração automática de endereço via DHCP. No SUSE Linux Enterprise Desktop, em que o NetworkManager está ativo por padrão, todas as placas de rede estão configuradas.

Também será necessário usar o DHCP se você estiver usando uma linha DSL sem nenhum IP estático atribuído pelo ISP (Internet Service Provider — Provedor de Serviços de Internet). Se você decidir usar o DHCP, configure os detalhes em *Opções do Cliente DHCP* na guia *Opções Globais* da caixa de diálogo *Configurações de Rede* do módulo de configuração de placa de rede do YaST. Se você tiver uma configuração de host virtual, em que hosts diferentes se comunicam pela mesma interface, será necessário um *Identificador de Cliente DHCP* para diferenciá-las.

O DHCP é uma boa opção para a configuração de clientes, mas não é a ideal para a configuração de servidores. Para definir um endereço IP estático, faça o seguinte:

1. Selecione uma placa na lista de placas detectadas na guia *Visão Geral* do módulo de configuração de placa de rede do YaST e clique em *Editar*.
2. Na guia *Endereço*, escolha *Endereço IP Atribuído Estaticamente*.
3. Digite o *Endereço IP*. Podem ser usados endereços IPv4 e IPv6. Digite a máscara de rede em *Máscara de Sub-rede*. Se for usado o endereço IPv6, use *Máscara de Sub-rede* para um comprimento do prefixo no formato `/64`.

Como opção, você pode digitar um *Nome de Host* completo para esse endereço, que será gravado no arquivo de configuração `/etc/hosts`.

4. Clique em *Avançar*.

5. Para ativar a configuração, clique em *OK*.

Se você usa o endereço estático, os servidores de nomes e o gateway padrão não são configurados automaticamente. Para configurar servidores de nomes, proceda conforme descrito em *Seção 20.4.1.4, "Configurando nome de host e DNS"*. Para configurar um gateway, proceda conforme descrito em *Seção 20.4.1.5, "Configurando o roteamento"*.

20.4.1.2.2 Configurando vários endereços

Um dispositivo de rede pode ter vários endereços IP.

Nota: álias são um recurso de compatibilidade

Os chamados álias ou rótulos, respectivamente, funcionam apenas com IPv4. Com IPv6, eles serão ignorados. O uso das interfaces de rede **`iproute2`** pode ter um ou mais endereços.

Ao usar o YaST para definir endereços adicionais para a sua placa de rede, faça o seguinte:

1. Selecione uma placa na lista de placas detectadas na guia *Visão Geral* da caixa de diálogo *Configurações de Rede* do YaST e clique em *Editar*.

2. Na guia *Endereço* › *Endereços Adicionais*, clique em *Adicionar*.

3. Digite o *Rótulo do Endereço IPv4*, o *Endereço IP* e a *Máscara de rede*. Não inclua o nome da interface no nome do álias.

4. Para ativar a configuração, confirme as definições.

20.4.1.2.3 Mudando o nome de dispositivo e as regras de udev

É possível mudar o nome de dispositivo da placa de rede quando ela for usada. Também é possível determinar se a placa de rede deve ser identificada pelo udev usando o endereço (MAC) de hardware ou o ID do barramento. A última opção é preferencial em servidores grandes para simplificar o hotplug de placas. Para definir essas opções com o YaST, faça o seguinte:

1. Selecione uma placa na lista de placas detectadas na guia *Visão Geral* da caixa de diálogo *Configurações de Rede* do YaST e clique em *Editar*.
2. Vá até a guia *Hardware*. O nome de dispositivo atual é mostrado em *Regras do Udev*. Clique em *Mudar*.
3. Selecione se o udev deve identificar a placa por seu *Endereço MAC* ou *ID do Bus*. O endereço MAC e o ID do barramento atuais da placa são mostrados na caixa de diálogo.
4. Para mudar o nome de dispositivo, marque a opção *Mudar Nome do Dispositivo* e edite o nome.
5. Para ativar a configuração, confirme as definições.

20.4.1.2.4 Mudando o driver do kernel da placa de rede

Para algumas placas de rede, vários drivers do Kernel podem estar disponíveis. Se a placa já estiver configurada, o YaST permitirá selecionar um driver do Kernel para uso na lista de drivers compatíveis disponíveis. É possível também especificar opções para o driver do Kernel. Para definir essas opções com o YaST, faça o seguinte:

1. Selecione uma placa na lista de placas detectadas na guia *Visão Geral* do módulo Configurações de Rede do YaST e clique em *Editar*.
2. Vá até a guia *Hardware*.
3. Selecione qual driver do Kernel usar em *Nome de Módulo*. Digite qualquer opção para o driver selecionado em *Opções*, usando o formato `opção=valor`. Se forem usadas mais opções, elas deverão ser separadas por espaços.
4. Para ativar a configuração, confirme as definições.

20.4.1.2.5 Ativando o dispositivo de rede

Se você usar o método com o **`wicked`**, poderá configurar seu dispositivo para ser iniciado durante o boot, na conexão a cabo, ao detectar a placa, manualmente ou nunca. Para mudar a inicialização do dispositivo, faça o seguinte:

1. No YaST, selecione uma placa na lista de placas detectadas em *Dispositivos de Rede* › *Configurações de Rede* e clique em *Editar*.
2. Na guia *Geral*, selecione a entrada desejada em *Ativação de Dispositivo*.
   Escolha *Em Tempo de Boot* para iniciar o dispositivo durante o boot do sistema. Com a opção *Em Conexão Cabo*, a interface é monitorada quanto a qualquer conexão física existente. Com a opção *Em Hotplug*, a interface é definida tão logo fique disponível. Ela se assemelha à opção *Em Tempo de Boot*, a única diferença é que não ocorre nenhum erro quando a interface não está presente no momento do boot. Escolha *Manualmente* para controlar a interface manualmente com **`ifup`**. Escolha *Nunca* para não iniciar o dispositivo. A opção *Em NFSroot* assemelha-se a *Em tempo de Boot*, mas a interface não é encerrada com o comando **`systemctl stop wicked.service`**. Use-a se você estiver usando um sistema de arquivos raiz NFS ou iSCSI.
3. Para ativar a configuração, confirme as definições.

20.4.1.2.6 Configurando o tamanho da unidade máxima de transferência

Você pode definir uma unidade máxima de transferência (MTU) para a interface. A MTU refere-se ao maior tamanho de pacote permitido, em bytes. Uma MTU maior proporciona melhor eficiência da largura de banda. No entanto, pacotes grandes podem bloquear uma interface lenta por algum tempo, aumentando a latência dos pacotes seguintes.

1. No YaST, selecione uma placa na lista de placas detectadas em *Dispositivos de Rede* › *Configurações de Rede* e clique em *Editar*.
2. Na guia *Geral*, selecione a entrada desejada na lista *Definir MTU*.
3. Para ativar a configuração, confirme as definições.

20.4.1.2.7 Configuração de Infiniband para IPoIB (InfiniBand sobre IP)

1. No YaST, selecione o dispositivo InfiniBand em *Dispositivos de Rede* › *Configurações de Rede* e clique em *Editar*.
2. Na guia *Geral*, selecione um dos modos IPoIB (*IP-over-InfiniBand* – InfiniBand sobre IP): *connected* (conectado, que é o padrão) ou *datagram* (datagrama).
3. Para ativar a configuração, confirme as definições.

Para obter mais informações sobre o InfiniBand, consulte `/usr/src/linux/Documentation/infiniband/ipoib.txt`.

20.4.1.2.8 Configurando o firewall

Sem precisar inserir a configuração de firewall detalhada como descrito na *Book "Security Guide" 15 "Masquerading and Firewalls" 15.4.1 "Configuring the Firewall with YaST"*, você pode determinar a configuração de firewall básica para seu dispositivo como parte da configuração dele. Proceda da seguinte maneira:

1. Abra o módulo *Dispositivos de Rede* › *Configurações de Rede* do YaST. Na guia *Visão Geral*, selecione uma placa na lista de placas detectadas e clique em *Editar*.
2. Acesse a guia *Geral* da caixa de diálogo *Configurações de Rede*.
3. Determine a *Zona de Firewall* à qual sua interface deve ser atribuída. As seguintes opções estão disponíveis:

   Firewall Desabilitado

   Essa opção fica disponível apenas quando o firewall está desabilitado, sem entrar em execução. Use esta opção apenas se a sua máquina pertencer a uma rede maior protegida por um firewall externo.

   Zona Atribuída Automaticamente

   Essa opção fica disponível apenas quando o firewall está habilitado. O firewall está em execução e a interface é atribuída automaticamente a uma zona de firewall. Para uma interface como essa, será usada a zona que contiver a palavra-chave `any` ou a zona externa.

Zona Interna (Desprotegida)

O firewall está em execução, mas não assegura o uso obrigatório de nenhuma regra para proteger a interface. Use esta opção se a sua máquina pertencer a uma rede maior protegida por um firewall externo. Ela também é útil para as interfaces conectadas à rede interna, quando a máquina possui mais interfaces de rede.

Zona Desmilitarizada

Zona desmilitarizada é uma linha de defesa adicional situada na frente de uma rede interna e da Internet (hostil). Os hosts designados a essa zona podem ser acessados a partir da rede interna e a Internet, mas não podem acessar a rede interna.

Zona Externa

O firewall está em execução nesta interface e a protege totalmente contra outros tráfegos de rede (provavelmente hostis). Ela é a opção padrão.

4. Para ativar a configuração, confirme as definições.

20.4.1.3 Configurando uma placa de rede não detectada

Se uma placa de rede não for detectada corretamente, ela não será incluída na lista de placas detectadas. Se você tiver certeza de que o sistema contém um driver para sua placa, poderá configurá-la manualmente. Se for possível, configure também tipos especiais de dispositivos de rede, como ponte, ligação, TUN ou TAP. Para configurar uma placa de rede não detectada (ou um dispositivo especial), faça o seguinte:

1. Na caixa de diálogo *Dispositivos de Rede* › *Configurações de Rede* › *Visão Geral* no YaST, clique em *Adicionar*.

2. Na caixa de diálogo *Hardware*, defina o *Tipo de Dispositivo* da interface entre as opções disponíveis e o *Nome de Configuração*. Se a placa de rede for um dispositivo PCMCIA ou USB, ative a respectiva caixa de seleção e saia dessa caixa de diálogo com *Avançar*. Do contrário, você poderá definir o *Nome de Módulo* do Kernel para usar na placa, e as respectivas *Opções*, se necessário.

Em *Opções do Ethtool*, você pode definir as opções de **`ethtool`** usadas pelo **`ifup`** para a interface. Consulte a página de manual de **`ethtool`** para conhecer as opções disponíveis. Se a string opcional iniciar com um `-` (por exemplo `-K nome_da_interface rx on`), a segunda palavra da string será substituída pelo nome da interface atual. Caso contrário (por exemplo `autoneg off speed 10`), **`ifup`** precederá `-s nome_da_interface`.

3. Clique em *Avançar*.
4. Configure quaisquer opções que forem necessárias, como o endereço IP, a ativação do dispositivo ou a zona de firewall da interface nas guias *Geral*, *Endereço* e *Hardware*. Para obter mais informações sobre as opções de configuração, consulte a *Seção 20.4.1.2, "Mudando a configuração de uma placa de rede"*.
5. Se você selecionou *Wireless* como o tipo de dispositivo da interface, configure a conexão wireless na próxima caixa de diálogo.
6. Para ativar a nova configuração de rede, confirme as definições.

20.4.1.4 Configurando nome de host e DNS

Se você não mudou a configuração de rede durante a instalação e a placa Ethernet já estava disponível, um nome de host foi gerado automaticamente para o seu computador e o DHCP foi ativado. O mesmo se aplica às informações de serviço de nomes de que o host necessita para se integrar a um ambiente de rede. Se o DHCP for usado para a configuração de endereços de rede, a lista de servidores de nomes de domínio será preenchida automaticamente com os dados adequados. Se uma configuração estática for preferencial, defina esses valores manualmente.

Para mudar o nome do seu computador e ajustar a lista de pesquisa do servidor de nomes, faça o seguinte:

1. Vá para a guia *Configurações de Rede* › *Nome de host/DNS* no módulo *Dispositivos de Rede* no YaST.
2. Digite o *Nome de Host* e, se necessário, o *Nome de Domínio*. O domínio é especialmente importante quando a máquina é um servidor de correio eletrônico. Observe que o nome de host é global e aplica-se a todas as interfaces de rede definidas.
   Se você estiver usando o DHCP para obter um endereço IP, o nome de host do seu computador será definido automaticamente pelo DHCP. Convém desabilitar este comportamento ao conectar-se a outras redes, visto que elas podem atribuir nomes de host

diferentes, e a mudança de nome de host em tempo de execução pode confundir a área de trabalho gráfica. Para desabilitar o uso do DHCP para obter um endereço IP, desmarque *Trocar Nome de Host via DHCP*.

Atribuir Nome de Host a IP de Loopback associa seu nome de host ao endereço IP `127.0.0.2` (loopback) em `/etc/hosts`. Trata-se de uma opção útil quando você deseja que o nome de host seja sempre resolvível, mesmo sem uma rede ativa.

3. Em *Modificar Configuração do DNS*, selecione o modo como a configuração do DNS (servidores de nomes, lista de pesquisa, o conteúdo do arquivo `/etc/resolv.conf`) é modificada.

   Se a opção *Usar Política Padrão* for selecionada, a configuração será gerenciada pelo script **`netconfig`**, que funde os dados definidos estaticamente (com o YaST ou nos arquivos de configuração) com os dados obtidos dinamicamente (do cliente DHCP ou do NetworkManager). Essa política padrão é suficiente na maioria dos casos.

   Se a opção *Apenas Manualmente* for selecionada, **`netconfig`** não terá permissão para modificar o arquivo `/etc/resolv.conf`. Entretanto, esse arquivo pode ser editado manualmente.

   Se a opção *Política Personalizada* for selecionada, deverá ser especificada uma string de *Regra de Política Personalizada* definindo a política de fusão. A string consiste em uma lista de nomes de interface separados por vírgula, considerada como fonte válida de configurações. Além dos nomes completos de interface, também são permitidos curingas básicos para corresponder a várias interfaces. Por exemplo, `eth* ppp?` primeiramente encontrará todas as interfaces eth, depois, todas as interfaces de ppp0 a ppp9. Existem dois valores de política especiais que indicam como aplicar as configurações estáticas definidas no arquivo `/etc/sysconfig/network/config`:

   `STATIC`
   : É necessário fundir as configurações estáticas com as configurações dinâmicas.

   `STATIC_FALLBACK`
   : As configurações estáticas são usadas apenas quando não há nenhuma configuração dinâmica disponível.

   Para obter mais informações, consulte a página de manual de **`netconfig`**(8) (**`man 8 netconfig`**).

4. Digite os *Servidores de Nome* e preencha a lista *Pesquisa de Domínio*. Servidores de nomes devem ser especificados por endereços IP, como 192.168.1.116, e não por nomes de host. Os nomes especificados na guia *Pesquisa de Domínio* são nomes de domínio usados para resolver nomes de host sem um domínio especificado. Se for usada mais de uma *Pesquisa de Domínio*, separe os domínios por vírgulas ou espaços.

5. Para ativar a configuração, confirme as definições.

É possível também editar o nome de host usando o YaST da linha de comando. As mudanças feitas pelo YaST entram em vigor imediatamente (o que não acontece quando se edita o arquivo `/etc/HOSTNAME` manualmente). Para mudar o nome de host, use o seguinte comando:

```
yast dns edit hostname=hostname
```

Para mudar os servidores de nomes, use os seguintes comandos:

```
yast dns edit nameserver1=192.168.1.116
yast dns edit nameserver2=192.168.1.117
yast dns edit nameserver3=192.168.1.118
```

20.4.1.5 Configurando o roteamento

Para que sua máquina se comunique com outras máquinas e redes, é necessário fornecer informações de roteamento para que o tráfego de rede siga o caminho correto. Se o DHCP for usado, essas informações serão fornecidas automaticamente. Se uma configuração estática for usada, esses dados deverão ser adicionados manualmente.

1. No YaST, vá para *Configurações de Rede* › *Roteamento*.

2. Digite o endereço IP do *Gateway Padrão* (IPv4 e IPv6, se necessário). O gateway padrão corresponde a todos os destinos possíveis, mas se houver uma entrada da tabela de roteamento que corresponda ao endereço exigido, ela será usada no lugar da rota padrão, pelo Gateway Padrão.

3. É possível digitar mais entradas na *Tabela de Roteamento*. Digite o endereço IP do *Destino*, o endereço IP do *Gateway* e a *Máscara de Rede*. Selecione o *Dispositivo* pelo qual será roteado o tráfego para a rede definida (o sinal de menos significa qualquer dispositivo). Para omitir qualquer um desses valores, use o sinal de menos `-`. Para digitar um gateway padrão na tabela, use `padrão` no campo *Destino*.

   > **Nota**
   >
   > Se forem usadas mais rotas padrão, será possível especificar a opção métrica para determinar qual rota possui a prioridade mais alta. Para especificar a opção métrica, digite `- metric` *`número`* em *Opções*. A rota com a métrica mais alta será usada como padrão. Se o dispositivo de rede for desconectado, sua rota será removida e o dispositivo seguinte será usado. Entretanto, o Kernel atual não usa métrica no roteamento estático, apenas os daemons de roteamento, como `multipathd`, podem fazê-lo.

4. Se o sistema for um roteador, habilite *Encaminhamento IPv4* e *Encaminhamento IPv6* em *Configurações de Rede*, conforme necessário.

5. Para ativar a configuração, confirme as definições.

20.5 NetworkManager

O NetworkManager é a solução ideal para laptops e outros computadores portáteis. Com o NetworkManager, não é necessário preocupar-se em configurar interfaces de rede e alternar entre redes quando você estiver em trânsito.

20.5.1 NetworkManager e `wicked`

Entretanto, como o NetworkManager não é uma solução adequada para todos os casos, você ainda pode escolher entre o método de gerenciamento de conexões de rede controlado pelo `wicked` e o NetworkManager. Para gerenciar sua conexão de rede com o NetworkManager, habilite-o no módulo Configurações de Rede do YaST, conforme descrito na *Seção 22.2, "Habilitando ou desabilitando o NetworkManager"*, e configure suas conexões de rede com o NetworkManager. Para ver uma lista dos casos de uso e uma descrição detalhada de como configurar e usar o NetworkManager, consulte o *Capítulo 22, Usando o NetworkManager*.

Algumas diferenças entre o wicked e o NetworkManager:

Privilégios de `root`

Se você usa o NetworkManager para configurar a rede, poderá alternar, parar ou iniciar com facilidade a conexão de rede, a qualquer momento, de dentro do ambiente de área de trabalho usando um applet. O NetworkManager também permite mudar e configurar conexões de placa wireless sem exigir privilégios de `root`. Por esse motivo, o NetworkManager é a solução ideal para uma estação de trabalho móvel.

O **`wicked`** também oferece algumas maneiras de alternar, parar ou iniciar a conexão com ou sem a intervenção do usuário, como os dispositivos gerenciados pelo usuário. No entanto, privilégios de `root` sempre são exigidos para mudar ou configurar um dispositivo de rede. Isso normalmente é um problema para a computação móvel, na qual não é possível pré-configurar todas as possibilidades de conexão.

Tipos de conexões de rede

Tanto o **`wicked`** quanto o NetworkManager podem gerenciar conexões de rede com uma rede wireless (com acesso WEP, WPA-PSK e WPA-Enterprise) e redes com fio usando a configuração DHCP e estática. Eles também suportam conexão por discagem e VPN. Com o NetworkManager, é possível também conectar um modem de banda larga móvel (3G) ou configurar uma conexão DSL, o que não é possível com a configuração tradicional.

O NetworkManager tenta manter o computador conectado o tempo todo usando a melhor conexão disponível. Se o cabo da rede for desconectado por acidente, ele tentará reconectar. Ele é capaz de localizar a rede que tiver a melhor intensidade de sinal na lista de conexões wireless e usá-la automaticamente para uma conexão. Para obter a mesma funcionalidade com o **`wicked`**, são necessárias mais configurações.

20.5.2 Funcionalidade do NetworkManager e arquivos de configuração

As configurações individuais de conexão de rede criadas com o NetworkManager são armazenadas em perfis de configuração. As conexões do *sistema* configuradas com o NetworkManager ou o YaST são gravadas em `/etc/networkmanager/system-connections/*` ou em `/etc/sysconfig/network/ifcfg-*`. No GNOME, todas as conexões definidas pelo usuário são armazenadas no GConf.

Caso não haja nenhum perfil configurado, o NetworkManager criará um automaticamente com o nome `Auto $INTERFACE-NAME`. Isso é uma tentativa de fazer funcionar sem qualquer configuração para tantos casos quanto forem possíveis (com segurança). Se os perfis criados automaticamente não atenderem às suas necessidades, use as caixas de diálogo de configuração da conexão de rede, fornecidas pelo GNOME, para modificá-los conforme desejado. Para obter mais informações, consulte a *Seção 22.3, "Configurando conexões de rede"*.

20.5.3 Controlando e bloqueando recursos do NetworkManager

Em máquinas administradas centralmente, determinados recursos do NetworkManager poderão ser controlados ou desabilitados com o PolKit, por exemplo, se um usuário tiver permissão para modificar as conexões definidas pelo administrador ou para definir suas próprias configurações de rede. Para ver ou mudar as respectivas políticas do NetworkManager, inicie a ferramenta gráfica *Autorizações* para o PolKit. Na árvore do lado esquerdo, elas se encontram abaixo da entrada *network-manager-settings*. Para ver uma introdução sobre o PolKit e detalhes de como usá-lo, consulte o *Book "*Security Guide*" 9 "Authorization with PolKit"*.

20.6 Configurando uma conexão de rede manualmente

A configuração manual do software de rede deve ser a última alternativa. É recomendável usar o YaST. Entretanto, essas informações de base sobre a configuração de rede também podem ajudar você na utilização do YaST.

20.6.1 Configuração de rede com o **wicked**

A ferramenta e biblioteca chamada **wicked** dispõe de uma nova estrutura para configuração de rede.

Um dos desafios do gerenciamento de interface de rede tradicional é a mistura das diversas camadas de gerenciamento de rede em um único script ou, no máximo, em dois scripts diferentes, que interagem entre si de uma forma não muito bem definida, com efeitos colaterais difíceis de prever, limites e convenções obscuros, etc. Diversas camadas de soluções alternativas

especiais para uma variedade de cenários diferentes aumentam a carga de manutenção. Estão sendo usados protocolos de configuração de endereço que são implementados por meio de daemons como o dhcpcd, que pouco se interagem com o restante da infraestrutura. Esquemas de nomeação de interface ruins que exigem suporte pesado a udev são introduzidos para obter identificação persistente das interfaces.

A ideia do wicked é analisar o problema de várias maneiras. Nenhuma delas é totalmente inovadora, mas esperamos que, ao tentar reunir ideias de diferentes projetos, seja criada uma solução global melhor.

Uma abordagem é usar um modelo de cliente/servidor. Dessa forma, o wicked pode definir recursos padronizados para ações como configuração de endereço que se integrem bem à estrutura geral. Por exemplo, na configuração de endereço, o administrador pode solicitar que uma interface seja configurada por DHCP ou IPv4 zeroconf, e tudo o que o serviço de configuração de endereço faz é obter o aluguel de seu servidor e passá-lo adiante para o processo do servidor do wicked, que instala os endereços e as rotas solicitadas.

A outra abordagem para analisar o problema é impor o aspecto de organização em camadas. Para qualquer tipo de interface de rede, é possível definir um serviço dbus que configure a camada do dispositivo da interface de rede: VLAN, ponte, ligação ou dispositivo paravirtualizado. Uma funcionalidade comum, como a configuração de endereço, é implementada por serviços de junção, que são colocados em camadas sobre esses serviços específicos do dispositivo, sem ter que implementá-los especificamente.

A estrutura do wicked implementa esses dois aspectos usando uma variedade de serviços dbus, que são anexados a uma interface de rede de acordo com o seu tipo. Veja a seguir uma visão geral simples da hierarquia de objeto no wicked.

Cada interface de rede é representada por um objeto filho de `/org/opensuse/Network/Interfaces`. O nome do objeto filho é dado por seu ifindex. Por exemplo, a interface de loopback, que geralmente possui ifindex 1, é `/org/opensuse/Network/Interfaces/1`, a primeira interface Ethernet registrada é `/org/opensuse/Network/Interfaces/2`.

Cada interface de rede tem uma “classe” associada, que é usada para selecionar as interfaces dbus suportadas. Por padrão, cada interface de rede pertence à classe `netif`, e o wickedd anexa automaticamente todas as interfaces compatíveis com essa classe. Na implementação atual, isso inclui as seguintes interfaces:

org.opensuse.Network.Interface

Funções de interface de rede genéricas, como mover o link para cima ou para baixo, atribuir uma MTU, etc.

org.opensuse.Network.Addrconf.ipv4.dhcp,
org.opensuse.Network.Addrconf.ipv6.dhcp,
org.opensuse.Network.Addrconf.ipv4.auto,
org.opensuse.Network.Addrconf.ipv6.auto

Serviços de configuração de endereço para DHCP, IPv6 autoconf, IPv4 zeroconf, etc.

Além disso, as interfaces de rede podem exigir ou oferecer mecanismos de configuração especiais. Por exemplo, em um dispositivo Ethernet, convém ter recursos para controlar a velocidade do link, o descarregamento de checksum, etc. Para isso, os dispositivos Ethernet têm uma classe própria chamada `netif-ethernet`, que é uma subclasse de `netif`. Como consequência, as interfaces dbus atribuídas a uma interface Ethernet incluem todos os serviços relacionados anteriormente e mais o `org.opensuse.Network.Ethernet`, que é um serviço disponível apenas para os objetos pertencentes à classe `netif-ethernet`.

Semelhantemente, existem classes para tipos de interface como pontes, VLANs, ligações ou infinibands.

O modo como você interage com a interface que precisa ser criada primeiro, como a VLAN, que é, na verdade, uma interface de rede virtual que fica acima de um dispositivo Ethernet. Para isso tudo, o wicked define interfaces de fábrica, como `org.opensuse.Network.VLAN.Factory`. Esse tipo de interface de fábrica oferece uma única função que permite criar uma interface do tipo solicitado. Essas interfaces de fábrica são anexadas ao nó da lista `/org/opensuse/Network/Interfaces`.

20.6.1.1 Suporte atual

O **`wicked`** suporta:

- Back ends de arquivo de configuração para analisar os arquivos `/etc/sysconfig/network` no estilo SUSE e RedHat. Como o desenvolvimento é feito em uma instalação do SUSE, os arquivos do SUSE provavelmente são bem mais estáveis do que os do RedHat.
- Um back end de arquivo de configuração para representar a configuração da interface de rede em XML. A sintaxe evoluiu até chegar na que é usada pelo netcf.
- Ativação e encerramento de interfaces de rede “normais”, como Ethernet ou InfiniBand, além de VLAN, ponte e dispositivos de ligação. A ligação e ponte ainda podem apresentar alguns problemas.
- Wireless, ainda incompleto e limitado a uma rede.

- Um cliente DHCPv4 e um cliente DHCPv6 incorporados.
- Existe um código experimental que deve ajudar a ativar automaticamente as interfaces logo que um link é detectado.
- Uma implementação de leitor/gravador XML, que está longe de cumprir com todos os padrões, mas possui pouco volume e parece ser razoavelmente rápido. Ela vem com uma implementação parcial do XPath 1.0, que permite extrair informações de uma descrição de interface XML sem que você tenha que fazer nenhuma análise de XML.

20.6.1.2 Usando o **wicked**

No SUSE Linux Enterprise, o **wicked** será executado por padrão, se você não selecionar o NetworkManager. Caso você tenha que habilitá-lo, chame:

```
systemctl enable --force wicked.service
```

Isso habilita os serviços do wicked, cria o link do álias `network.service` com o álias `wicked.service` e inicia a rede na próxima inicialização.

Iniciando o processo do servidor:

```
systemctl start wickedd.service
```

Isso inicia o **wickedd** (o servidor principal) e os suplicantes associados no modo de depuração, imprimindo as informações de rastreamento no syslog:

```
/usr/sbin/wickedd --foreground
/usr/lib/wicked/bin/wickedd-dhcp4 --foreground
/usr/lib/wicked/bin/wickedd-auto4 --foreground
/usr/lib/wicked/bin/wickedd-dhcp6 --foreground
```

Ativando a rede:

```
systemctl start wicked.service
```

Se preferir, também com o álias `network.service`:

```
systemctl start network.service
```

Estes comandos usam as fontes de configuração padrão ou do sistema, conforme definido em `/etc/wicked/client.xml`.

Para habilitar a depuração, defina `WICKED_DEBUG_PARAM` em `/etc/sysconfig/network/config` (isso pode mudar no futuro), por exemplo:

```
WICKED_DEBUG_PARAM="--debug most"
```

Use o utilitário cliente para exibir as informações da interface para todas as interfaces ou para a interface especificada com *`ifname`*:

```
wicked show all
wicked show ifname
```

Na saída XML:

```
wicked show-xml all
wicked show-xml ifname
```

Ativando uma interface:

```
wicked ifup eth0
wicked ifup wlan0
...
```

Como não há nenhuma fonte de configuração especificada, o cliente do wicked verifica suas fontes de configuração padrão definidas em `/etc/wicked/client.xml`:

1. `firmware:` iBFT (iSCSI Boot Firmware Table)
2. `compat:` arquivos `ifcfg`, implementados para compatibilidade
3. `wicked:`*`CAMINHO`* formato de configuração XML nativo do wicked armazenado em *`CAMINHO`* (padrão: `/etc/wicked/ifconfig`)

O que o **`wicked`** obtiver destas fontes para determinada interface será aplicado. A ordem de importância pretendida é `firmware`, depois `compat` e depois `wicked`, isso poderá ser mudado no futuro, quando os requisitos de compatibilidade do ifcfg ficarem flexíveis.

Vamos apresentar algo interessante: um exemplo de interface VLAN:

```
wicked ifup --ifconfig ./samples/wicked/vlan-static.xml eth0.42
```

Isso deve ativar a interface VLAN chamada “eth0.42”, com uma tag VLAN de 42 e alguns endereços IP estaticamente atribuídos. Para ver se ela funciona, tente:

```
ip addr show
ip route show
```

O comando acima recupera a descrição de todas as interfaces do arquivo especificado e ativa a interface chamada “eth0.42”. Como o arquivo inclui apenas uma interface, você pode usar `all` (todas) no lugar do nome da interface. Como a palavra já diz, todas as interfaces listadas no arquivo são ativadas.

Para ativar uma única interface, o cliente executa vários métodos e argumentos do servidor usando elementos XML, solicitando ao servidor para mudar o estado da interface desejada para “ativado”. Esta operação criará a interface VLAN simultaneamente, se ainda não existir.

Use a mesma abordagem para baixar a interface:

```
wicked ifdown eth0.42
```

Para baixar e apagar a interface, use:

```
wicked ifdown --delete --ifconfig ./samples/wicked/vlan-static.xml eth0.42
```

Para obter mais informações, consulte a página de manual de **`wicked`**.

20.6.1.3 Ativando várias interfaces

Para ligações e pontes, convém definir a topologia inteira do dispositivo em um arquivo e ativá-la de uma vez. Isso é bastante útil principalmente para ligações, em que você talvez tenha que criar primeiro os dispositivos escravos (se forem dispositivos virtuais, como as VLANs).

Nesse tipo de cenário, defina a topologia do dispositivo em um arquivo e chame o wicked para ativar toda a configuração. Encontre um exemplo em `samples/wicked/bridge-static.xml` na documentação do pacote (`/usr/share/doc/packages/wicked`). Esta configuração define uma ponte Ethernet criada com base em duas interfaces VLAN. Para ativá-la, chame:

```
wicked ifup --ifconfig ./samples/wicked/bridge-static.xml all
```

O cliente ativa os dispositivos na ordem apropriada: criando primeiro as duas interfaces VLAN, depois a ponte e, por fim, adicionando as interfaces VLAN como portas à ponte.

20.6.1.4 Administrando mudanças incrementais

Com o **wicked**, não há necessidade de baixar uma interface para reconfigurá-la (exceto se exigido pelo Kernel). Por exemplo, para adicionar outro endereço IP ou rota a uma interface de rede estaticamente configurada, adicione o endereço IP à definição da interface e execute outra operação “ifup”. O servidor tentará de tudo para atualizar apenas as configurações que foram mudadas. Isso vale para as opções no nível do link, como a MTU do dispositivo ou o endereço MAC, e também para as configurações no nível da rede, como endereços, rotas ou até mesmo o modo de configuração de endereço (por exemplo, ao mover da configuração estática para DHCP).

Claro que as coisas se tornam mais complicadas quando há interfaces virtuais combinadas a vários dispositivos reais, como pontes ou ligações. Para dispositivos acoplados, é impossível mudar determinados parâmetros enquanto o dispositivo está ativado. Se você fizer isso, haverá erro.

No entanto, o que ainda deve funcionar é a adição ou remoção dos dispositivos filho de uma ligação ou ponte, ou a escolha de uma interface principal da ligação.

20.6.1.5 Extensões do wicked: configuração de endereço

O **wicked** foi desenvolvido para ser extensível com scripts shell. É possível definir as extensões no arquivo `config.xml`.

Atualmente, há várias classes diferentes de extensões suportadas:

- configuração de link: são scripts responsáveis por configurar a camada de link do dispositivo de acordo com a configuração fornecida pelo cliente e por desconfigurá-la novamente.
- configuração de endereço: são scripts responsáveis por gerenciar a configuração de endereço de um dispositivo. Geralmente, a configuração de endereço e o DHCP são gerenciados pelo próprio **wicked**, mas podem ser implementados por meio de extensões.
- extensão de firewall: estes scripts podem aplicar regras de firewall.

Normalmente, as extensões possuem um comando de início e parada, um “arquivo pid” opcional e um conjunto de variáveis de ambiente que são passadas para o script.

Para ilustrar como isso deve funcionar, observe a extensão de firewall definida em `etc/server.xml`:

```
<dbus-service interface="org.opensuse.Network.Firewall">
 <action name="firewallUp"   command="/etc/wicked/extensions/firewall up"/>
 <action name="firewallDown" command="/etc/wicked/extensions/firewall down"/>

 <!-- default environment for all calls to this extension script -->
 <putenv name="WICKED_OBJECT_PATH" value="$object-path"/>
 <putenv name="WICKED_INTERFACE_NAME" value="$property:name"/>
 <putenv name="WICKED_INTERFACE_INDEX" value="$property:index"/>
</dbus-service>
```

A extensão está anexada à interface do serviço dbus e define comandos a serem executados para as ações dessa interface. Além disso, a declaração pode definir e inicializar as variáveis de ambiente passadas para as ações.

20.6.1.6 Extensões do wicked: arquivos de configuração

É possível estender a administração de arquivos de configuração também com scripts. Por exemplo, as atualizações DNS dos aluguéis são definitivamente administradas pelo script `extensions/resolver`, com o comportamento configurado em `server.xml`:

```
<system-updater name="resolver">
 <action name="backup" command="/etc/wicked/extensions/resolver backup"/>
 <action name="restore" command="/etc/wicked/extensions/resolver restore"/>
 <action name="install" command="/etc/wicked/extensions/resolver install"/>
 <action name="remove" command="/etc/wicked/extensions/resolver remove"/>
</system-updater>
```

Quando uma atualização chega ao `wickedd`, as rotinas do atualizador do sistema analisam o aluguel e chamam os comandos apropriados (`backup`, `install`, etc.) no script do resolver. Isso, por sua vez, define as configurações DNS usando **`/sbin/netconfig`** ou manualmente, gravando `/etc/resolv.conf` como fallback.

20.6.2 Arquivos de configuração

Esta seção fornece uma visão geral dos arquivos de configuração de rede e explica sua finalidade e formato usado.

20.6.2.1 `/etc/sysconfig/network/ifcfg-*`

Estes arquivos contêm as configurações tradicionais das interfaces de rede.

Nota: `wicked` e os arquivos `ifcfg-*`

O **`wicked`** lerá estes arquivos se você especificar o modo de compatibilidade com o prefixo `compat:` ao usar a opção `--ifconfig`. De acordo com a configuração padrão do SUSE Linux Enterprise Server 12 no `/etc/wicked/client.xml`, o **`wicked`** lê esses arquivos antes dos arquivos de configuração XML em `/etc/wicked/ifconfig`.

Os arquivos `ifcfg-*` incluem informações, como o modo de início e o endereço IP. Os parâmetros possíveis são descritos na página de manual de `ifup`. Além disso, a maioria das variáveis dos arquivos `dhcp` e `wireless` poderá ser usada nos arquivos `ifcfg-*` se uma configuração geral for usada para apenas uma interface. Entretanto, a maioria das variáveis de `/etc/sysconfig/network/config` é global e não pode ser anulada em arquivos ifcfg. Por exemplo, as variáveis `NETWORKMANAGER` ou `NETCONFIG_*` são globais.

Para configurar as interfaces `macvlan` e `macvtab`, consulte as páginas de manual de `ifcfg-macvlan` e `ifcfg-macvtap`. Por exemplo, para a interface macvlan, insira `ifcfg-macvlan0` com as seguintes configurações:

```
STARTMODE='auto'
MACVLAN_DEVICE='eth0'
#MACVLAN_MODE='vepa'
#LLADDR=02:03:04:05:06:aa
```

Para saber sobre o `ifcfg.template`, consulte a *Seção 20.6.2.2, "/etc/sysconfig/network/config, /etc/sysconfig/network/dhcp e /etc/sysconfig/network/wireless"*.

20.6.2.2 /etc/sysconfig/network/config, /etc/sysconfig/network/dhcp e /etc/sysconfig/network/wireless

O arquivo `config` contém configurações gerais para o comportamento de **`ifup`**, **`ifdown`** e **`ifstatus`**. `dhcp` contém configurações para DHCP e `wireless` para placas de rede local wireless. Nos três arquivos de configuração, as variáveis estão em forma de comentário. Algumas das variáveis de `/etc/sysconfig/network/config` também podem ser usadas nos arquivos `ifcfg-*`, nos quais recebem prioridade mais alta. O arquivo `/etc/sysconfig/network/ifcfg.template` lista as variáveis que podem ser especificadas para cada interface. Entretanto, a maioria das variáveis de `/etc/sysconfig/network/config` é global e não pode ser anulada em arquivos ifcfg. Por exemplo, as variáveis `NETWORKMANAGER` ou `NETCONFIG_*` são globais.

20.6.2.3 /etc/sysconfig/network/routes e /etc/sysconfig/network/ifroute-*

O roteamento estático dos pacotes TCP/IP é determinado pelos arquivos `/etc/sysconfig/network/routes` e `/etc/sysconfig/network/ifroute-*`. Todas as rotas estáticas exigidas pelas várias tarefas do sistema podem ser especificadas em `/etc/sysconfig/network/routes`: rotas para um host, rotas para um host via gateway e rotas para uma rede. Para cada interface que precisa de roteamento individual, defina um arquivo de configuração adicional: `/etc/sysconfig/network/ifroute-*`. Substitua o curinga (`*`) pelo nome da interface. As entradas nos arquivos de configuração de roteamento terão esta aparência:

```
# Destination     Gateway           Netmask           Interface  Options
```

O destino da rota está na primeira coluna. Essa coluna pode conter o endereço IP de uma rede ou host ou, no caso de servidores de nomes *acessíveis*, o nome completo da rede ou do host. A rede deve ser gravada em notação CIDR (endereço com o comprimento do prefixo de roteamento associado), como 10.10.0.0/16 para rotas IPv4 ou fc00::/7 para rotas IPv6. A palavra-chave `default` indica que a rota é o gateway padrão na mesma família de endereços do gateway. Para dispositivos sem gateway, use destinos explícitos 0.0.0.0/0 ou ::/0.

A segunda coluna contém o gateway padrão ou um gateway por meio do qual um host ou uma rede podem ser acessados.

A terceira coluna foi descontinuada; ela antes incluía a máscara de rede IPv4 do destino. Para rotas IPv6, rota padrão ou ao usar o comprimento do prefixo (notação CIDR) na primeira coluna, digite um traço (`-`) aqui.

A quarta coluna contém o nome da interface. Se você a deixar vazia usando um traço (`-`), poderá provocar um comportamento não intencional em `/etc/sysconfig/network/routes`. Para obter mais informações, consulte a página de manual de `routes`.

Uma quinta coluna (opcional) pode ser usada para inserir opções especiais. Para obter detalhes, consulte a página de manual de `routes`.

EXEMPLO 20.5 INTERFACES DE REDE COMUNS E ALGUMAS ROTAS ESTÁTICAS

```
# --- IPv4 routes in CIDR prefix notation:
# Destination     [Gateway]         -                   Interface
127.0.0.0/8       -                 -                   lo
204.127.235.0/24  -                 -                   eth0
default           204.127.235.41    -                   eth0
207.68.156.51/32  207.68.145.45     -                   eth1
192.168.0.0/16    207.68.156.51     -                   eth1

# --- IPv4 routes in deprecated netmask notation"
# Destination     [Dummy/Gateway]   Netmask             Interface
#
127.0.0.0         0.0.0.0           255.255.255.0       lo
204.127.235.0     0.0.0.0           255.255.255.0       eth0
default           204.127.235.41    0.0.0.0             eth0
207.68.156.51     207.68.145.45     255.255.255.255     eth1
192.168.0.0       207.68.156.51     255.255.0.0         eth1

# --- IPv6 routes are always using CIDR notation:
# Destination     [Gateway]               -           Interface
2001:DB8:100::/64 -                       -           eth0
```

```
2001:DB8:100::/32 fe80::216:3eff:fe6d:c042 -          eth0
```

20.6.2.4 /etc/resolv.conf

O domínio ao qual o host pertence está especificado em `/etc/resolv.conf` (palavra-chave `search`). É possível especificar até seis domínios com um total de 256 caracteres com a opção `search`. Durante a resolução de um nome incompleto, uma tentativa de gerar um nome será feita, anexando as entradas de `pesquisa` individuais. É possível especificar até 3 servidores de nomes com a opção `nameserver`, cada um em sua própria linha. Os comentários são precedidos por cerquilha ou ponto-e-vígula (`#` ou `;`). Como um exemplo, consulte o *Exemplo 20.6, "/etc/resolv.conf"*.

Entretanto, o `/etc/resolv.conf` não deve ser editado manualmente. Isso porque ele é gerado pelo script **`netconfig`**. Para definir configurações DNS estáticas sem usar o YaST, edite as variáveis apropriadas manualmente no arquivo `/etc/sysconfig/network/config`:

`NETCONFIG_DNS_STATIC_SEARCHLIST`
: lista de nomes de domínios DNS usados para pesquisa de nomes de host

`NETCONFIG_DNS_STATIC_SERVERS`
: lista de endereços IP de servidor de nomes usados para pesquisa de nomes de host

`NETCONFIG_DNS_FORWARDER`
: o nome do encaminhador de DNS que precisa ser configurado, por exemplo `bind` ou `resolver`

`NETCONFIG_DNS_RESOLVER_OPTIONS`
: opções arbitrárias que serão gravadas em `/etc/resolv.conf`, por exemplo:

```
debug attempts:1 timeout:10
```

Para obter mais informações, consulte a página de manual de `resolv.conf`.

`NETCONFIG_DNS_RESOLVER_SORTLIST`
: lista com até 10 itens, por exemplo:

```
130.155.160.0/255.255.240.0 130.155.0.0
```

Para obter mais informações, consulte a página de manual de `resolv.conf`.

Para desabilitar a configuração do DNS usando o netconfig, defina `NETCONFIG_DNS_POLICY=''`. Para obter mais informações sobre o **`netconfig`**, consulte a página de manual de `netconfig(8)` (**`man 8 netconfig`**).

EXEMPLO 20.6 `/etc/resolv.conf`

```
# Our domain
search example.com
#
# We use dns.example.com (192.168.1.116) as nameserver
nameserver 192.168.1.116
```

20.6.2.5 `/sbin/netconfig`

O **`netconfig`** é uma ferramenta modular destinada a gerenciar configurações de rede adicionais. Ele funde as configurações definidas estaticamente com as configurações fornecidas pelos mecanismos de configuração automática, como DHCP ou PPP, de acordo com uma política predefinida. As mudanças necessárias são aplicadas ao sistema chamando-se os módulos do netconfig responsáveis pela modificação de um arquivo de configuração e pela reinicialização de um serviço ou uma ação semelhante.

O **`netconfig`** reconhece três ações principais. Os comandos **`netconfig modify`** e **`netconfig remove`** são usados por daemons, como DHCP ou PPP, para fornecer ou remover configurações do netconfig. Apenas o comando **`netconfig update`** está disponível para o usuário:

`modify`

O comando **`netconfig modify`** modifica as configurações dinâmicas específicas de interface e serviço, além de atualizar a configuração da rede. O netconfig lê as configurações da entrada padrão ou de um arquivo especificado pela opção `--lease-file` *`nome_de_arquivo`* e as armazena internamente até a próxima reinicialização do sistema (ou a próxima ação modify ou remove). As configurações que já existirem para a mesma combinação de interface e serviço serão sobregravadas. A interface é especificada pelo parâmetro `-i` *`nome_da_interface`*. O serviço é especificado pelo parâmetro `-s` *`nome_do_serviço`*.

`remove`

O comando **`netconfig remove`** remove as configurações dinâmicas fornecidas por uma ação modificadora para a combinação de interface e serviço especificada, além de atualizar a configuração da rede. A interface é especificada pelo parâmetro `-i` *`nome_da_interface`*. O serviço é especificado pelo parâmetro `-s` *`nome_do_serviço`*.

`update`

O comando **`netconfig update`** atualiza a configuração da rede usando as configurações atuais. Isso é útil quando a política ou a configuração estática é mudada. Use o parâmetro `-m` *`tipo_de_módulo`* se desejar atualizar apenas um serviço especificado (`dns`, `nis` ou `ntp`).

A política do netconfig e as configurações estáticas são definidas manualmente ou por meio do YaST no arquivo `/etc/sysconfig/network/config`. As configurações dinâmicas fornecidas pelas ferramentas de configuração automática, como DHCP ou PPP, são entregues diretamente por essas ferramentas com as ações **`netconfig modify`** e **`netconfig remove`**. Quando o NetworkManager está habilitado, o netconfig (no modo de política `auto`) usa apenas as configurações do NetworkManager, ignorando as configurações de qualquer outra interface configurada pelo método tradicional ifup. Se o NetworkManager não fornecer nenhuma configuração, as configurações estáticas serão usadas como fallback. Não há suporte para a utilização mista do NetworkManager nem para o método **`wicked`**.

Para obter mais informações sobre o **`netconfig`**, consulte **`man 8 netconfig`**.

20.6.2.6 `/etc/hosts`

Neste arquivo, mostrado em *Exemplo 20.7, "`/etc/hosts`"*, os endereços IP foram atribuídos a nomes de host. Se nenhum servidor de nomes for implementado, todos os hosts nos quais uma conexão IP for configurada precisarão ser listados aqui. Para cada host, digite uma linha no arquivo com o endereço IP, o nome completo do host e o nome de host. O endereço IP precisa estar no início da linha e as entradas separadas por espaços vazios e guias. Comentários são sempre precedidos pelo sinal `#`.

EXEMPLO 20.7 `/etc/hosts`

```
127.0.0.1 localhost
192.168.2.100 jupiter.example.com jupiter
192.168.2.101 venus.example.com venus
```

20.6.2.7 /etc/networks

Aqui, os nomes de rede são convertidos em endereços de rede. O formato é semelhante ao do arquivo `hosts`, exceto que os nomes de rede precedem os endereços. Consulte o *Exemplo 20.8, "/etc/networks"*.

EXEMPLO 20.8 `/etc/networks`

```
loopback    127.0.0.0
localnet    192.168.0.0
```

20.6.2.8 /etc/host.conf

Resolução de nomes — a conversão de nomes de host e de rede através da biblioteca *resolver* é controlada por esse arquivo. Esse arquivo é usado somente para programas vinculados a libc4 ou libc5. Para programas glibc atuais, consulte as configurações em `/etc/nsswitch.conf`. Um parâmetro precisa estar sempre independente em sua própria linha. Comentários são precedidos pelo sinal `#`. A *Tabela 20.2, "Parâmetros para /etc/host.conf"* mostra os parâmetros disponíveis. Uma amostra de `/etc/host.conf` é mostrada no *Exemplo 20.9, "/etc/host.conf"*.

TABELA 20.2 PARÂMETROS PARA /ETC/HOST.CONF

order *hosts*, *bind*	Especifica em que ordem os serviços são acessados para a resolução de nomes. Os argumentos disponíveis são (separados por espaços vazios ou vírgulas):
	hosts: pesquisa o arquivo `/etc/hosts`
	bind: acessa um servidor de nomes
	nis: usa o NIS
multi *on/off*	Define se um host digitado em `/etc/hosts` pode ter vários endereços IP.
nospoof *on* spoofalert *on/off*	Esses parâmetros influenciam o *spoof* do servidor de nomes, mas não exercem qualquer influência na configuração da rede.

trim *domainname*	O nome de domínio especificado será separado do nome de host após a resolução de nome de host (desde que o nome de host inclua o nome de domínio). Essa opção é útil apenas quando os nomes do domínio local estão no arquivo `/etc/hosts`, mas ainda devem ser reconhecidos com os nomes de domínio anexados.

EXEMPLO 20.9 `/etc/host.conf`

```
# We have named running
order hosts bind
# Allow multiple address
multi on
```

20.6.2.9 `/etc/nsswitch.conf`

O lançamento do GNU C Library 2.0 foi acompanhado pelo lançamento do *NSS* (Name Service Switch). Consulte a página de manual do `nsswitch.conf(5)` e *The GNU C Library Reference Manual* (Manual de Referência da Biblioteca GNU C) para obter mais detalhes.

A ordem das consultas é definida no arquivo `/etc/nsswitch.conf`. Uma amostra do `nsswitch.conf` é mostrada no *Exemplo 20.10, "/etc/nsswitch.conf"*. Comentários são precedidos pelo sinal `#`. Nesse exemplo, a entrada no banco de dados `hosts` significa que uma solicitação foi enviada para `/etc/hosts` (`arquivos`) através do DNS.

EXEMPLO 20.10 `/etc/nsswitch.conf`

```
passwd:     compat
group:      compat

hosts:      files dns
networks:   files dns

services:   db files
protocols:  db files
rpc:        files
```

```
ethers:     files
netmasks:   files
netgroup:   files nis
publickey:  files

bootparams: files
automount:  files nis
aliases:    files nis
shadow:     compat
```

Os “bancos de dados” disponíveis em NSS estão listados na *Tabela 20.3, “Bancos de dados disponíveis por /etc/nsswitch.conf”*.
As opções de configuração para bancos de dados NSS estão listadas na *Tabela 20.4, “Opções de configuração para bancos de dados “NSS””*.

TABELA 20.3 BANCOS DE DADOS DISPONÍVEIS POR /ETC/NSSWITCH.CONF

`aliases`	Álias de correio implementados por `sendmail`; consulte **`man`** `5 aliases`.
`ethers`	Endereços de Ethernet.
`netmasks`	Lista de redes e suas máscaras de sub-rede. Apenas necessário quando se usa sub-redes.
`group`	Para grupos de usuários usados por `getgrent`. Consulte também a página de manual para **`group`**.
`hosts`	Para nomes de host e endereços IP, usados por `gethostbyname` e funções similares.
`netgroup`	Listas de usuários e hosts válidos na rede com a finalidade de controlar permissões de acesso, consulte a página de manual do `netgroup(5)`.
`networks`	Nomes e endereços de redes, usados por `getnetent`.

`publickey`	Chaves públicas e secretas de Secure_RPC usadas pelo NFS e NIS+.
`passwd`	Senhas de usuários, usadas por `getpwent`; consulte a página de manual do `passwd(5)`.
`protocols`	Protocolos de rede, usados por `getprotoent`; consulte a página de manual do `protocols(5)`.
`rpc`	Nomes e endereços de RPC (Remote Procedure Call) usados por `getrpcbyname` e funções similares.
`services`	Serviços de rede, usados por `getservent`.
`shadow`	Senhas transitórias de usuários, usadas por `getspnam`; consulte a página de manual do `shadow(5)`.

TABELA 20.4 OPÇÕES DE CONFIGURAÇÃO PARA BANCOS DE DADOS "NSS"

`files`	arquivos de acesso direto, por exemplo, `/etc/aliases`
`db`	acesso através de um banco de dados
`nis`, `nisplus`	NIS, consulte também o *Book "*Security Guide*" 3 "Using NIS"*
`dns`	só pode ser usada como extensão de `hosts` e `networks`
`compat`	só pode ser usada como extensão de `passwd`, `shadow` e `group`

20.6.2.10 /etc/nscd.conf

Esse arquivo é usado para configurar o nscd (name service cache daemon). Consulte as páginas de manual de `nscd(8)` e `nscd.conf(5)`. Por padrão, as entradas do sistema de `passwd` e `groups` são armazenadas em cache pelo nscd. Isso é importante para o desempenho de serviços de diretório, como NIS e LDAP, pois, caso contrário, a conexão de rede precisaria ser usada para cada acesso a nomes ou grupos. `hosts` não é armazenado em cache por padrão, porque o mecanismo no nscd para armazenar hosts em cache impede o sistema local de confiar em verificações de pesquisa forward e reverse. Em vez de solicitar ao nscd para armazenar nomes em cache, configure um servidor DNS para armazenamento em cache.

Se o armazenamento em cache de `passwd` estiver ativado, normalmente levará quinze segundos para que um usuário local recentemente adicionado seja reconhecido. Reduza este tempo de espera reiniciando o nscd com:

```
systemctl restart nscd.service
```

20.6.2.11 /etc/HOSTNAME

`/etc/HOSTNAME` contém o FQHN (fully qualified host name – nome completo do host). O nome completo do host é o nome de host com o nome de domínio anexado. Este arquivo deve incluir apenas uma linha (na qual o nome de host é definido). Ele é lido durante a inicialização da máquina.

20.6.3 Testando a configuração

Antes de gravar sua configuração nos arquivos de configuração, você pode testá-la. Para definir uma configuração de teste, use o comando **`ip`**. Para testar a conexão, use o comando **`ping`**.

O comando **`ip`** muda a configuração de rede diretamente, sem gravá-la no arquivo de configuração. A menos que você insira a configuração nos arquivos de configuração corretos, a configuração de rede mudada será perdida na reinicialização.

Nota: `ifconfig` e `route` obsoletos

As ferramentas **`ifconfig`** e **`route`** estão obsoletas. Em vez disso, use **`ip`**. O **`ifconfig`**, por exemplo, limita os nomes de interface a 9 caracteres.

20.6.3.1 Configurando uma interface de rede com **ip**

ip é uma ferramenta para mostrar e configurar dispositivos de rede, roteamentos, roteamento de políticas e túneis.

ip é uma ferramenta muito complexa. Sua sintaxe comum é **ip** *opções objeto comando*. Você pode trabalhar com os seguintes objetos:

link
: Este objeto representa um dispositivo de rede.

address
: Este objeto representa o endereço IP do dispositivo.

neighbor
: Este objeto representa uma entrada de cache ARP ou NDISC.

route
: Este objeto representa a entrada da tabela de roteamento.

rule
: Este objeto representa uma regra no banco de dados de políticas de roteamento.

maddress
: Este objeto representa um endereço multicast.

mroute
: Este objeto representa uma entrada de cache de roteamento multicast.

tunnel
: Este objeto representa um túnel sobre IP.

Se nenhum comando for fornecido, será usado o comando padrão (normalmente **list**).

Mude o estado de um dispositivo com o comando **ip link set** *nome_do_dispositivo comando*. Por exemplo, para desativar o dispositivo eth0, digite **ip link set** `eth0 down`. Para ativá-lo novamente, use **ip link set** `eth0 up`.

Após ativar um dispositivo, você poderá configurá-lo. Para definir o endereço IP, use **ip addr add** *endereço_ip* + `dev` *nome_do_dispositivo*. Por exemplo, para definir o endereço da interface eth0 como 192.168.12.154/30 com o broadcast padrão (opção `brd`), digite **ip addr** `add 192.168.12.154/30 brd + dev eth0`.

Para ter uma conexão ativa, você também precisa configurar o gateway padrão. Para definir um gateway para o sistema, digite **ip route add** `endereço_ip_do_gateway`. Para traduzir um endereço IP para outro, use **nat**: **ip route add nat** `endereço_ip` **via** `outro_endereço_ip`.

Para exibir todos os dispositivos, use **ip link ls**. Para exibir apenas as interfaces em execução, use **ip link ls up**. Para imprimir as estatísticas de interface de um dispositivo, digite **ip -s link ls** `nome_do_dispositivo`. Para ver os endereços dos dispositivos, digite **ip addr**. Na saída do comando **ip addr**, você também pode encontrar informações sobre os endereços MAC dos dispositivos. Para mostrar todas as rotas, use **ip route show**.

Para obter mais informações sobre como usar o **ip**, digite **ip** `help` ou consulte a página de manual de `ip(8)`. A opção `help` também está disponível para todos os subcomandos **ip**. Se, por exemplo, você precisar de ajuda para **ip** `addr`, digite **ip** `addr help`. Encontre o manual do **ip** em `/usr/share/doc/packages/iproute2/ip-cref.pdf`.

20.6.3.2 Testando uma conexão com o comando ping

O comando **ping** é a ferramenta padrão para testar o funcionamento de uma conexão TCP/IP. Ele usa o protocolo ICMP para enviar um pequeno pacote de dados, o datagrama ECHO_REQUEST, para o host de destino, solicitando uma resposta imediata. Se isso funcionar, o **ping** exibirá uma mensagem nesse sentido. Isso indica que o link da rede está funcionando.

O **ping** vai além de simplesmente testar a função da conexão entre dois computadores; ele também fornece algumas informações básicas sobre a qualidade da conexão. No *Exemplo 20.11, "Saída do comando ping"*, você pode ver um exemplo da saída do **ping**. A penúltima linha contém informações sobre o número de pacotes transmitidos, o número de pacotes perdidos e o tempo total da execução do **ping**.

Como destino, é possível usar um nome de host ou endereço IP, por exemplo, **ping** `exemplo.com` ou **ping** `192.168.3.100`. O programa enviará pacotes até que você pressione Ctrl–C.

Se você só precisar verificar a funcionalidade da conexão, poderá limitar o número dos pacotes com a opção `-c`. Por exemplo, para limitar o ping a três pacotes, digite **ping** `-c 3 exemplo.com`.

EXEMPLO 20.11 SAÍDA DO COMANDO PING

```
ping -c 3 example.com
PING example.com (192.168.3.100) 56(84) bytes of data.
```

```
64 bytes from example.com (192.168.3.100): icmp_seq=1 ttl=49 time=188 ms
64 bytes from example.com (192.168.3.100): icmp_seq=2 ttl=49 time=184 ms
64 bytes from example.com (192.168.3.100): icmp_seq=3 ttl=49 time=183 ms
--- example.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 183.417/185.447/188.259/2.052 ms
```

O intervalo padrão entre dois pacotes é um segundo. Para mudar o intervalo, o ping fornece a opção `-i`. Por exemplo, para aumentar o intervalo do ping para dez segundos, digite **`ping`** `-i 10 exemplo.com`.

Em um sistema com vários dispositivos de rede, às vezes é útil enviar o ping através de um endereço de interface específico. Para isso, use a opção `-I` com o nome do dispositivo selecionado, por exemplo, **`ping`** `-I wlan1 exemplo.com`.

Para obter mais opções e informações sobre como usar o ping, digite **`ping`** `-h` ou consulte a página de manual de `ping (8)`.

Dica: Executando ping em endereços IPv6

Para endereços IPv6, use o comando **`ping6`**. Observe que, para executar ping em endereços locais de link, deve-se especificar a interface com `-I`. O comando a seguir funcionará se o endereço for acessível via `eth1`:

```
ping6 -I eth1 fe80::117:21ff:feda:a425
```

20.6.4 Arquivos unit e scripts de inicialização

Além dos arquivos de configuração descritos anteriormente, há os arquivos unit do systemd e vários scripts que carregam os serviços de rede durante a inicialização da máquina. Eles são iniciados assim que o sistema passa para o destino `multi-user.target`. Alguns desses arquivos unit e scripts estão descritos em *Alguns arquivos unit e scripts de inicialização para programas de rede*. Para obter mais informações sobre o `systemd`, consulte o *Capítulo 11, O daemon* `systemd`, e para mais informações sobre os destinos do `systemd`, consulte a página de manual de `systemd.special` (**`man systemd.special`**).

`network.target`

`network.target` é o destino do systemd para projeto de rede, mas seu significado depende das configurações fornecidas pelo administrador do sistema.

Para obter mais informações, consulte http://www.freedesktop.org/wiki/Software/systemd/NetworkTarget/.

`multi-user.target`

`multi-user.target` é o destino do systemd para um sistema multiusuários com todos os serviços de rede necessários.

`xinetd.service`

Inicia o xinetd. O xinetd pode ser usado para disponibilizar os serviços do servidor no sistema. Por exemplo, ele pode iniciar o vsftpd sempre que uma conexão FTP for inicializada.

`rpcbind.service`

Inicia o utilitário rpcbind, que converte os números de programa RPC em endereços universais. Necessário para os serviços RPC, como um servidor NFS.

`ypserv.service`

Inicia o servidor NIS.

`ypbind.service`

Inicia o cliente NIS.

`/etc/init.d/nfsserver`

Inicia o servidor NFS.

`/etc/init.d/postfix`

Controla o processo de postfix.

20.7 Configurando dispositivos de ligação

Em alguns sistemas, existe a necessidade de implementar conexões de rede compatíveis com outros requisitos além dos padrões de disponibilidade ou segurança de dados de um dispositivo Ethernet comum. Nesses casos, vários dispositivos Ethernet podem ser agregados a um único dispositivo de ligação.

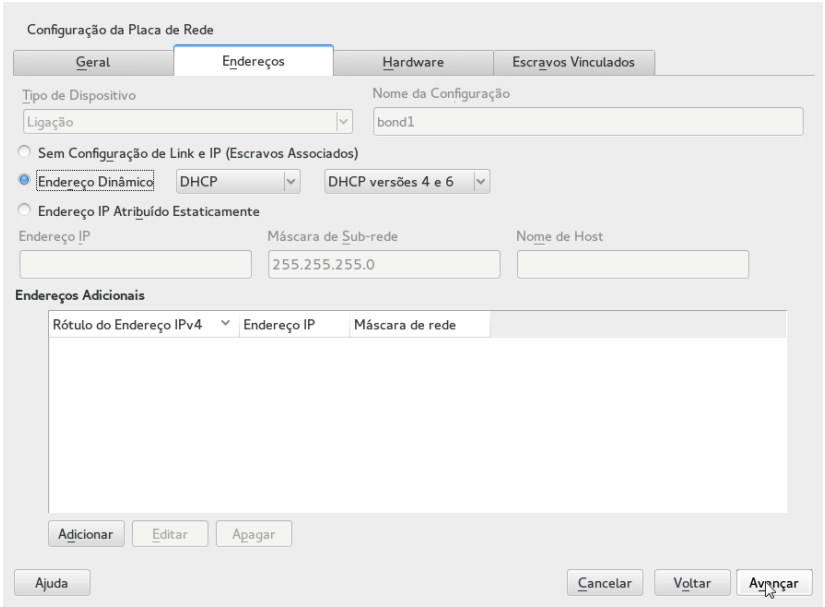
A configuração do dispositivo de ligação é feita através das opções dos módulos de ligação. O comportamento é afetado principalmente pelo modo do dispositivo de ligação. Por padrão, o modo é `mode=active-backup`, o que significa que um dispositivo escravo diferente será ativado se houver falha no escravo ativo.

Dica: Ligação e Xen

O uso de dispositivos de ligação só é interessante para máquinas que tenham várias placas de rede reais disponíveis. Na maioria das configurações, isso significa que você deve usar a configuração de ligação apenas no Dom0. Somente se você tiver várias placas de rede atribuídas a um sistema Convidado VM é que também poderá ser útil configurar a ligação em um Convidado VM.

Para configurar um dispositivo de ligação, siga este procedimento:

1. Execute *YaST* › *Dispositivos de Rede* › *Configurações de Rede*.
2. Use *Adicionar* e mude o *Tipo de Dispositivo* para *Ligação*. Continue com *Avançar*.



3. Escolha como vai atribuir o endereço IP ao dispositivo de ligação. Há três métodos à sua disposição:

- Nenhum Endereço IP
- Endereço Dinâmico (com DHCP ou Zeroconf)
- Endereço IP atribuído estaticamente

Use o método mais apropriado ao seu ambiente.

4. Na guia *Escravos Vinculados*, selecione os dispositivos Ethernet que devem ser incluídos na ligação ativando as caixas de seleção relacionadas.
5. Edite as *Opções do Driver de Vinculação*. Os seguintes modos estão disponíveis para configuração:

   - balance-rr
   - active-backup
   - balance-xor
   - broadcast
   - 802.3ad
     `802.3ad` é o modo LACP padronizado de "Agregação de links dinâmicos do IEEE 802.3ad".
   - balance-tlb
   - balance-alb

6. Verifique se o parâmetro `miimon=100` foi adicionado às *Opções do Driver de Vinculação*. Sem esse parâmetro, a integridade dos dados não é verificada regularmente.
7. Clique em *Avançar* e saia do YaST clicando em *OK* para criar o dispositivo.

Todos os modos, e muito mais opções, são explicados em detalhes no *Linux Ethernet Bonding Driver HOWTO* encontrado em `/usr/src/linux/Documentation/networking/bonding.txt` após a instalação do pacote `kernel-source`.

20.7.1 Hotplug de escravos associados

Em ambientes de rede específicos (como os de Alta Disponibilidade), há casos em que você precisa substituir uma interface de escravo associado por outra. O motivo pode ser uma falha constante no dispositivo de rede. A solução é configurar o hotplug dos escravos associados.

A ligação é configurada como de costume (de acordo com **`man 5 ifcfg-bonding`**), por exemplo:

```
ifcfg-bond0
          STARTMODE='auto' # or 'onboot'
          BOOTPROTO='static'
          IPADDR='192.168.0.1/24'
          BONDING_MASTER='yes'
          BONDING_SLAVE_0='eth0'
          BONDING_SLAVE_1='eth1'
          BONDING_MODULE_OPTS='mode=active-backup miimon=100'
```

Os escravos são especificados com `STARTMODE=hotplug` e `BOOTPROTO=none`:

```
ifcfg-eth0
          STARTMODE='hotplug'
          BOOTPROTO='none'

ifcfg-eth1
          STARTMODE='hotplug'
          BOOTPROTO='none'
```

`BOOTPROTO=none` usa as opções de ethtool (quando fornecidas), mas não define o link ativo no **`ifup eth0`**. O motivo é que a interface do escravo é controlada pelo master de ligação.

`STARTMODE=hotplug` faz com que a interface do escravo se una à ligação automaticamente assim que estiver disponível.

As regras do `udev` em `/etc/udev/rules.d/70-persistent-net.rules` precisam ser mudadas para corresponder ao dispositivo pelo ID do barramento (udev palavra-chave `KERNELS` igual a "SysFS BusID" como visível em **`hwinfo --netcard`**), e não pelo endereço MAC, para permitir a substituição do hardware com defeito (uma placa de rede no mesmo slot, mas com um MAC diferente) e evitar confusão conforme a ligação modifica o endereço MAC de todos os seus escravos.

Por exemplo:

```
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
KERNELS=="0000:00:19.0", ATTR{dev_id}=="0x0", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth0"
```

No momento da inicialização, o `network.service` do systemd não espera o hotplug dos escravos, mas sim a ligação ficar pronta, o que requer no mínimo um escravo disponível. Quando uma das interfaces dos escravos é removida (desvincular do driver NIC, **`rmmod`** do driver NIC ou remoção do hotplug do PCI verdadeira) do sistema, o kernel a remove automaticamente da ligação. Quando uma nova placa é adicionada ao sistema (substituição do hardware no slot), o `udev` a renomeia usando a regra de nome persistente baseada em barramento com o nome do escravo e chama o **`ifup`** para ela. A chamada do **`ifup`** une-a automaticamente à ligação.

21 Sincronização de horário com NTP

O mecanismo NTP (network time protocol) é um protocolo para sincronizar o horário do sistema na rede. Primeiro, uma máquina pode obter o horário de um servidor, que é uma fonte de horário confiável. Segundo, a máquina pode agir como uma fonte de horário para outros computadores na rede. O objetivo é duplo: manter o tempo absoluto e a sincronização do horário do sistema de todas as máquinas na rede.

Manter um horário exato do sistema é importante em várias situações. Geralmente, o relógio do hardware incorporado não atende aos requisitos dos aplicativos, como bancos de dados ou clusters. A correção manual do horário do sistema levaria a problemas severos pois, por exemplo, um pulo inverso pode causar o mau funcionamento de aplicativos críticos. Em uma rede, geralmente é necessário sincronizar o horário do sistema de todas as máquinas, porém, o ajuste manual do horário não é um bom método. O NTP dispõe de um mecanismo para resolver esses problemas. O serviço NTP ajusta continuamente o horário do sistema com a ajuda de servidores de horário confiáveis na rede. Ele habilita também o gerenciamento de relógios de referência local como relógios controlados pelo rádio.

Nota

Para habilitar a sincronização de horário por meio do diretório ativo, siga as instruções no .

21.1 Configurando um cliente NTP com YaST

O daemon do NTP (`ntpd`) que acompanha o pacote `ntp` vem predefinido para usar o relógio do computador como a referência de horário. Entretanto, o uso do relógio do hardware só serve como fallback nos casos em que não há uma fonte de horário mais precisa disponível. O YaST simplifica a configuração de um cliente NTP.

21.1.1 Configuração Básica

A configuração do cliente NTP do YaST (*Serviços de Rede* › *Configuração NTP*) é composta por guias. Defina o modo de iniciar do `ntpd` e o servidor para consulta na guia *Configurações Gerais*.

Apenas Manualmente

Selecione *Apenas Manualmente* para iniciar manualmente o daemon `ntpd`.

Agora e ao Inicializar

Selecione *Agora e ao Inicializar* para iniciar o `ntpd` automaticamente quando o sistema for inicializado. Essa configuração é altamente recomendada.

21.1.2 Mudando a configuração básica

Os servidores e outras fontes de horário para a consulta do cliente estão listados na guia *Configurações Gerais*. Modifique esta lista conforme necessário com *Adicionar*, *Editar* e *Apagar*. *Exibir Registro* fornece a possibilidade de exibir os arquivos de registro do seu cliente.

Clique em *Adicionar* para adicionar uma nova fonte de informação de horário. Na caixa de diálogo seguinte, selecione o tipo de fonte com a qual a sincronização de horário deve ser realizada. As seguintes opções estão disponíveis:

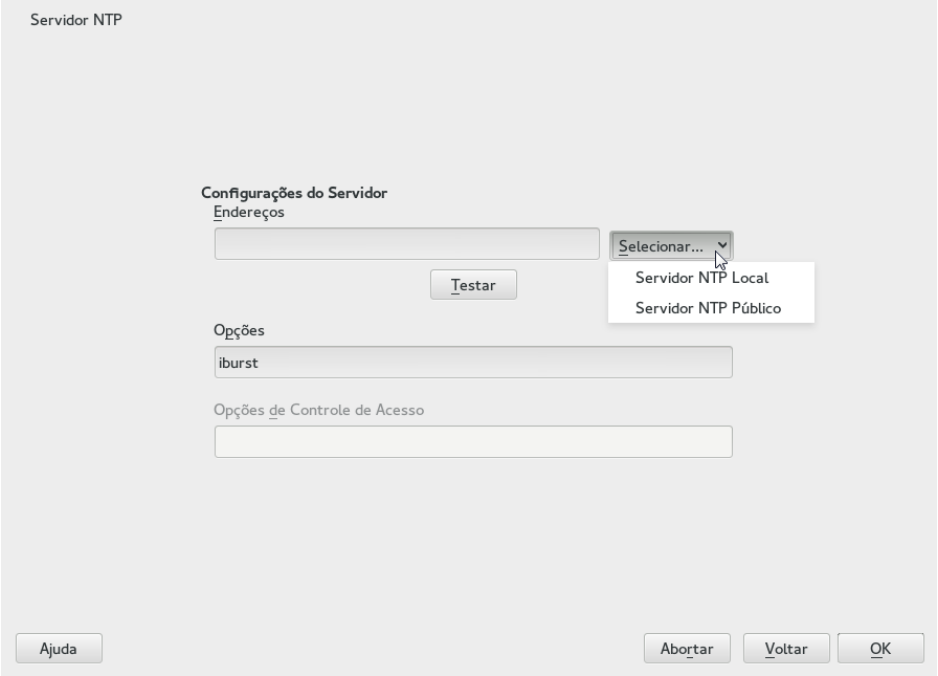


FIGURA 21.1 YAST: SERVIDOR NTP

Servidor

Na lista suspensa *Selecionar* (veja a *Figura 21.1, "YaST: servidor NTP"*), determine se é para configurar a sincronização de horário usando um servidor de horário da rede local (*Servidor NTP Local*) ou um servidor de horário baseado na Internet que controla o seu fuso horário

(*Servidor NTP Público*). Para um servidor de horário local, clique em *Busca* para iniciar uma consulta SLP por servidores de horário disponíveis na sua rede. Selecione o servidor de horário mais adequado a partir da lista de resultados de pesquisa e saia da caixa de diálogo com *OK*. Para um servidor de horário público, selecione o país (fuso horário) e um servidor adequado da lista sob *Servidor NTP Público*, em seguida, saia da caixa de diálogo com *OK*. Na caixa de diálogo principal, teste a disponibilidade do servidor selecionado com *Testar*. *Opções* permite que você especifique opções adicionais para o `ntpd`.

Com o uso de *Opções de Controle de Acesso*, você pode restringir as ações que o computador remoto pode desempenhar com o daemon em execução no seu computador. Esse campo apenas será habilitado após marcar *Restringir Serviço NTP Apenas aos Servidores Configurados* na guia *Configurações de Segurança* (veja a *Figura 21.2, "Configuração NTP Avançada: Configurações de Segurança"*). As opções correspondem às cláusulas `restrict` em `/etc/ntp.conf`. Por exemplo, `nomodify notrap noquery` não permite que o servidor modifique as configurações de NTP do seu computador e use o recurso de detecção (um recurso de registro de eventos remotos) do seu daemon NTP. O uso dessas restrições é recomendado para os servidores fora de controle (por exemplo, na Internet).

Consulte `/usr/share/doc/packages/ntp-doc` (parte do pacote `ntp-doc`) para obter informações detalhadas.

Peer

Um peer é uma máquina com a qual é estabelecido um relacionamento simétrico: ele atua como servidor de horário e como cliente. Para usar um peer na mesma rede em vez de um servidor, digite o endereço do sistema. O restante da caixa de diálogo é igual à caixa de diálogo *Servidor*.

Relógio controlado pelo rádio

Para usar um relógio controlado pelo rádio no seu sistema para a sincronização de horário, insira o tipo de relógio, o número da unidade, o nome do dispositivo e outras opções nesta caixa de diálogo. Clique em *Calibração do Driver* para ajustar o driver. Informações detalhadas sobre a operação de um rádio relógio local estão disponíveis em `/usr/share/doc/packages/ntp-doc/html/refclock.htm`.

Transmissão de saída

Consultas e informações sobre horário também podem ser transmitidas na rede. Nesta caixa de diálogo, insira o endereço ao qual estas transmissões devem ser enviadas. Não ative a transmissão a menos que você tenha uma fonte de horário confiável como um relógio controlado por rádio.

Transmissão de entrada

Se você deseja que o seu cliente receba suas informações através de transmissão, insira o endereço do qual os respectivos pacotes devem ser aceitos nestes campos.

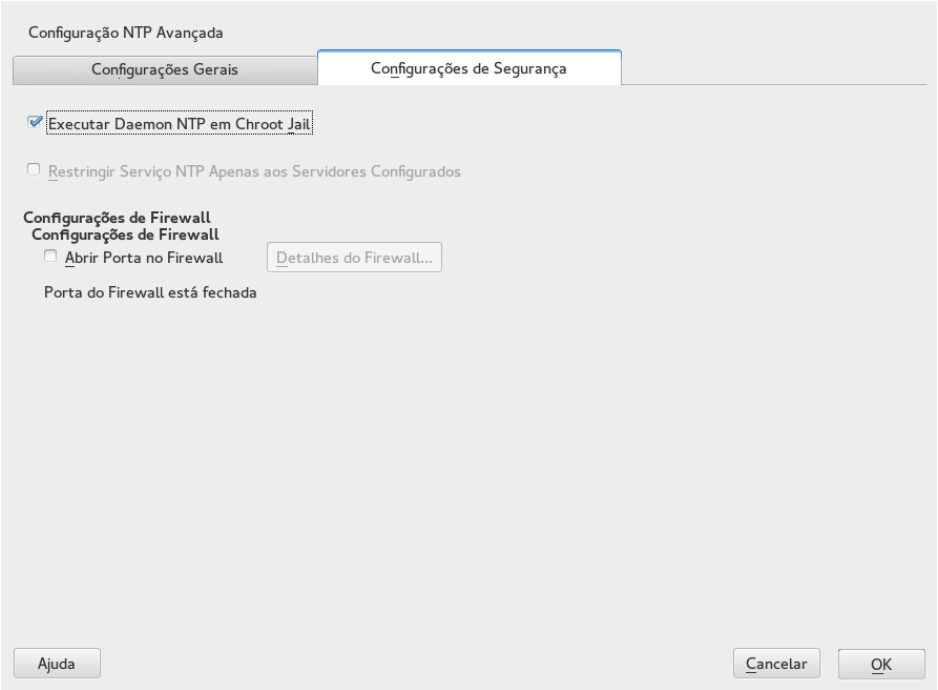


FIGURA 21.2 CONFIGURAÇÃO NTP AVANÇADA: CONFIGURAÇÕES DE SEGURANÇA

Na guia *Configurações de Segurança* (veja a *Figura 21.2, "Configuração NTP Avançada: Configurações de Segurança"*), determine se o `ntpd` deve ser iniciado em um chroot jail. Por padrão, a opção *Executar Daemon NTP em Chroot Jail* está ativada. Isso aumenta a segurança em caso de ataque ao `ntpd`, já que impede o invasor de comprometer todo o sistema.

Restringir Serviço NTP Apenas aos Servidores Configurados aumenta a segurança do seu sistema ao não permitir que os computadores remotos vejam e modifiquem as configurações de NTP do seu computador e que usem o recurso de detecção para o registro de eventos remotos. Depois de habilitadas, as restrições serão aplicadas a todos os computadores remotos, exceto se você anular as opções de controle de acesso para computadores individuais na lista de fontes de horário na guia *Configurações Gerais*. Para todos os outros computadores remotos, só é permitida a consulta de horário local.

Habilite *Abrir Porta no Firewall* se o SuSEFirewall2 estiver ativo (que é o padrão). Se você manter a porta fechada, não será possível estabelecer uma conexão com o servidor de horário.

21.2 Configurando manualmente o NTP na rede

A forma mais fácil de usar um servidor de horário na rede é definir parâmetros de servidor. Por exemplo, se um servidor de horário denominado `ntp.exemplo.com` estiver acessível na rede, adicione seu nome ao arquivo `/etc/ntp.conf` incluindo a seguinte linha:

```
server ntp.example.com
```

Para adicionar mais servidores de horário, insira linhas adicionais com a palavra-chave `server`. Após a inicialização do `ntpd` com o comando **`systemctl start ntp.service`**, levará cerca de uma hora para estabilizar o horário e criar o arquivo drift que corrige o relógio do computador local. Com o arquivo de descompasso, o erro sistemático do relógio do hardware pode ser computado assim que o computador for ligado. A correção é usada imediatamente, resultando em uma estabilidade maior do horário do sistema.

Há duas maneiras possíveis de usar o mecanismo NTP como cliente: primeiro, o cliente pode consultar o horário a partir de um servidor conhecido em intervalos regulares. Com vários clientes, esta abordagem pode causar uma carga alta no servidor. Segundo, o cliente pode esperar por transmissões de NTP enviadas por servidores de horário de transmissão na rede. Esta abordagem tem a desvantagem de que a qualidade do servidor é desconhecida e um servidor transmitindo a informação errada pode causar problemas graves.

Se o horário for obtido através de uma transmissão, você não precisará do nome do servidor. Neste caso, insira a linha `broadcastclient` no arquivo de configuração `/etc/ntp.conf`. Para usar um ou mais servidores de horário conhecidos exclusivamente, insira seus nomes na linha iniciando com `servers`.

21.3 Sincronização de horário dinâmica em tempo de execução

Se o sistema for inicializado sem conexão de rede, o `ntpd` será iniciado, mas não conseguirá resolver os nomes DNS dos servidores de horário definidos no arquivo de configuração. Isso poderá acontecer se você usar o NetworkManager com Wi-Fi criptografado.

Para que o `ntpd` resolva os nomes DNS em tempo de execução, defina a opção `dynamic`. Em seguida, quando a rede é estabelecida algum tempo após a inicialização, o `ntpd` procura os nomes novamente e acessa os servidores de horário para capturar a hora.

Edite manualmente o `/etc/ntp.conf` e adicione `dynamic` a uma ou mais entradas `server`:

```
server ntp.example.com dynamic
```

Se preferir, use o YaST e faça o seguinte:

1. No YaST, clique em *Serviços de Rede* › *Configuração NTP*.
2. Selecione o servidor que deseja configurar. Em seguida, clique em *Editar*.
3. Ative o campo *Opções* e adicione `dynamic`. Separe-o por um espaço, se já houver outras opções digitadas.
4. Clique em *OK* para fechar a caixa de diálogo de edição. Repita a etapa anterior para mudar todos os servidores conforme desejado.
5. Por fim, clique em *OK* para gravar as configurações.

21.4 Configurando um relógio de referência local

O pacote de software `ntpd` inclui drivers para conexão de relógios locais de referência. Uma lista de relógios suportados está disponível no pacote `ntp-doc` no arquivo `/usr/share/doc/packages/ntp-doc/html/refclock.htm`. Cada driver está associado a um número. No NTP, a configuração real é feita por pseudos endereços IP. Os relógios são inseridos no arquivo `/etc/ntp.conf` como se existissem na rede. Para este propósito, endereços IP especiais são atribuídos a eles no formato `127.127.`*`t`*`.`*`u`*. Aqui, *`t`* representa o tipo de relógio e determina o driver a ser usado e *`u`* representa a unidade, que determina a interface usada.

Normalmente, os drivers individuais têm parâmetros especiais que descrevem detalhes de configuração. O arquivo `/usr/share/doc/packages/ntp-doc/drivers/driver`*`NN`*`.html` (onde *`NN`* é o número do driver) fornece informações sobre o tipo específico de relógio. Por exemplo, o relógio “type 8” (relógio controlado por rádio na interface serial) exige um modo adicional que especifica o relógio de forma mais precisa. O módulo de recebimento Conrad DCF77, por exemplo, tem o modo 5. Para usar este relógio como referência preferida, especifique a palavra-chave `prefer`. A linha do `servidor` completa para um módulo de recebimento Conrad DCF77 seria:

```
server 127.127.8.0 mode 5 prefer
```

Outros relógios seguem o mesmo padrão. Após a instalação do pacote `ntp-doc`, a documentação do NTP fica disponível no diretório `/usr/share/doc/packages/ntp-doc`. O arquivo `/usr/share/doc/packages/ntp-doc/refclock.html` fornece links para as páginas que descrevem os parâmetros do driver.

22 Usando o NetworkManager

O NetworkManager é a solução ideal para laptops e outros computadores portáteis. Ele suporta tipos e padrões de criptografia avançados para conexões de rede, incluindo conexões com rede protegidas por 802.1X. 802.1X é o “Padrão IEEE para Redes Locais e de Área Metropolitana — Controle de Acesso a Rede Baseado na Porta”. Com o NetworkManager, você não precisa se preocupar em configurar interfaces de rede nem em alternar entre redes wireless ou com fio quando estiver em trânsito. O NetworkManager pode conectar-se automaticamente a redes wireless conhecidas ou gerenciar várias conexões de rede paralelamente, caso em que a conexão mais rápida é usada como padrão. Além disso, você pode alternar manualmente entre as redes disponíveis e gerenciar sua conexão de rede usando um applet na bandeja do sistema.

Várias conexões podem estar ativas simultaneamente, em vez de apenas uma. Isso lhe permite desplugar o laptop de uma Ethernet e permanecer conectado por uma conexão wireless.

22.1 Casos de uso para o NetworkManager

O NetworkManager dispõe de uma interface do usuário sofisticada e intuitiva, que permite aos usuários alternar facilmente seu ambiente de rede. Contudo, o NetworkManager não é uma solução adequada nos seguintes casos:

- O computador fornece serviços de rede para outros computadores de sua rede, por exemplo, se ele for um servidor DHCP ou DNS.
- Seu computador é um servidor Xen ou seu sistema é um sistema virtual dentro do Xen.

22.2 Habilitando ou desabilitando o NetworkManager

Em laptops, o NetworkManager está habilitado por padrão. No entanto, ele pode ser habilitado ou desabilitado a qualquer momento no módulo Configurações de Rede do YaST.

1. Execute o YaST e vá para *Dispositivos de Rede* › *Configurações de Rede*.
2. A caixa de diálogo *Configurações de Rede* é aberta. Vá até a guia *Opções Globais*.

3. Para configurar e gerenciar suas conexões de rede com o NetworkManager:

    a. No campo *Método de Configuração da Rede*, selecione *Controlado por Usuário com o NetworkManager*.

    b. Clique em *OK* e feche o YaST.

    c. Configure as conexões de rede com o NetworkManager, conforme descrito na *Seção 22.3, "Configurando conexões de rede"*.

4. Para desativar o NetworkManager e controlar a rede com sua própria configuração

    a. No campo *Método de Configuração da Rede*, escolha *Controlled by wicked* (Controlado pelo wicked).

    b. Clique em *OK*.

    c. Configure a placa de rede com o YaST usando a configuração automática através do DHCP ou de um endereço IP estático.
    Há uma descrição detalhada da configuração de rede com o YaST na *Seção 20.4, "Configurando uma conexão de rede com o YaST"*.

22.3 Configurando conexões de rede

Após habilitar o NetworkManager no YaST, configure suas conexões de rede com o front end do NetworkManager disponível no GNOME. Ele mostra guias para todos os tipos de conexões de rede; por exemplo, conexões com fio, wireless, de banda larga móvel, DSL e VPN.

Para abrir a caixa de diálogo de configuração de rede no GNOME, abra o menu de configurações, pelo menu de status, e clique na entrada *Rede*.

Nota: disponibilidade das opções

Dependendo da configuração de seu sistema, talvez não seja permitido configurar conexões. Em um ambiente seguro, talvez algumas opções estejam bloqueadas ou exijam permissão de `root`. Consulte o administrador do sistema para obter os detalhes.

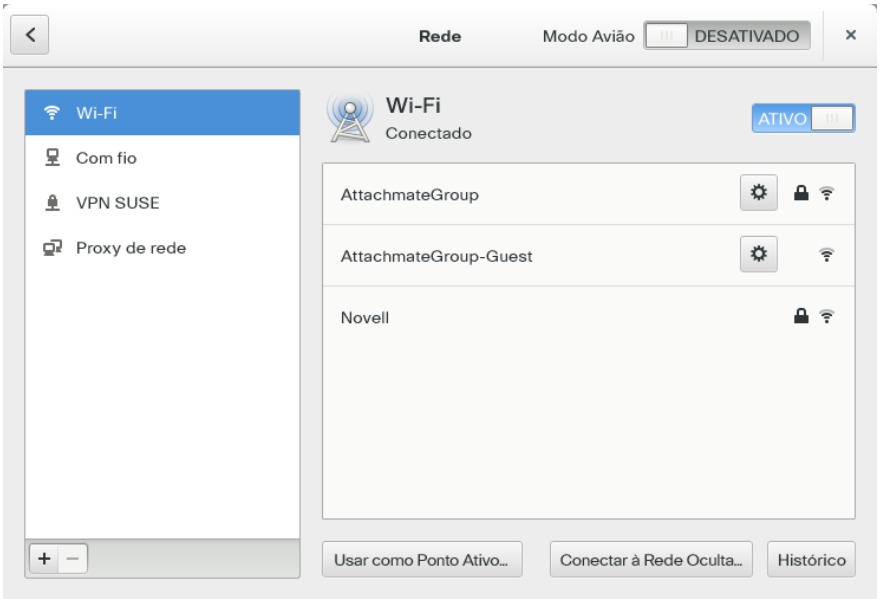


FIGURA 22.1 CAIXA DE DIÁLOGO CONEXÕES DE REDE DO GNOME

PROCEDIMENTO 22.1 ADICIONANDO E EDITANDO CONEXÕES

1. Abra a caixa de diálogo de configuração do NetworkManager.
2. Para adicionar uma conexão:
    a. Clique no ícone de + no canto inferior esquerdo.
    b. Selecione o tipo de conexão preferencial e siga as instruções.
    c. Ao concluir, clique em *Adicionar*.
    d. Depois de confirmadas as mudanças, a conexão de rede recém-configurada será exibida na lista de redes disponíveis que aparece ao abrir o Menu de Status.
3. Para editar uma conexão:
    a. Selecione a entrada para editar.
    b. Clique no ícone de engrenagem para abrir a caixa de diálogo *Configurações da Conexão*.
    c. Faça as mudanças e clique em *Aplicar* para gravá-las.

d. Para disponibilizá-la como conexão do sistema, vá para a guia *Identidade* e marque a caixa de seleção *Make available to other users* (Disponibilizar para outros usuários). Para obter mais informações sobre Conexões de Usuário e Sistema, consulte a *Seção 22.4.1, "Conexões de usuário e sistema"*

22.3.1 Gerenciando conexões de rede com fio

Se o seu computador estiver conectado a uma rede com fio, use o applet do NetworkManager para gerenciar a conexão.

1. Abra o Menu de Status e clique em *Com fio* para mudar os detalhes da conexão ou desligá-la.
2. Para mudar as configurações, clique em *Wired Settings* (Configurações com Fio) e clique no ícone de engrenagem.
3. Para desligar todas as conexões de rede, ative a configuração *Airplane Mode* (Modo Avião).

22.3.2 Gerenciando conexões de rede wireless

As redes wireless visíveis estão listadas no menu do applet do NetworkManager do GNOME em *Redes Wireless*. A força do sinal de cada rede também é mostrada no menu. Redes wireless criptografadas são marcadas com um ícone de escudo.

PROCEDIMENTO 22.2 CONECTANDO-SE A UMA REDE WIRELESS VISÍVEL

1. Para conectar-se a uma rede wireless visível, abra o Menu de Status e clique em *Wi-Fi*.
2. Clique em *Turn On* (Ativar) para habilitá-la.
3. Clique em *Select Network* (Selecionar Rede), selecione a Rede Wi-Fi e clique em *Conectar*.
4. Se a rede estiver criptografada, será aberta uma caixa de diálogo de configuração. Ela mostra o tipo de criptografia que a rede usa e as caixas de texto para digitar as credenciais de login.

PROCEDIMENTO 22.3 CONECTANDO-SE A UMA REDE WIRELESS INVISÍVEL

1. Para conectar-se a uma rede que não transmite seu identificador do conjunto de serviços (SSID ou ESSID) e, portanto, não pode ser detectada automaticamente, abra o Menu de Status e clique em *Wi-Fi*.
2. Clique em *Configurações Wi-Fi* para abrir o menu de configurações detalhadas.
3. Verifique se o seu Wi-Fi está habilitado e clique em *Conectar a uma Rede Oculta...*.
4. Na caixa de diálogo aberta, digite o SSID ou o ESSID em *Nome de Rede* e defina os parâmetros de criptografia, se necessário.

Uma rede wireless escolhida explicitamente permanecerá conectada o máximo de tempo possível. Se houver um cabo de rede conectado durante esse período, todas as conexões definidas como *Stay connected when possible* (Permanecer conectado quando possível) ficarão conectadas enquanto a conexão wireless continuar ativa.

22.3.3 Configurando a placa Wi-Fi/Bluetooth como ponto de acesso

Se a placa Wi-Fi/Bluetooth suportar o modo de ponto de acesso, você poderá usar o NetworkManager para a configuração.

1. Abra o Menu de Status e clique em *Wi-Fi*.
2. Clique em *Configurações Wi-Fi* para abrir o menu de configurações detalhadas.
3. Clique em *Use as Hotspot...* (Usar como Ponto Ativo) e siga as instruções.
4. Use as credenciais mostradas na caixa de diálogo resultante para conectar-se ao ponto ativo de uma máquina remota.

22.3.4 NetworkManager e VPN

O NetworkManager suporta várias tecnologias de VPN (Virtual Private Network). Para cada tecnologia, o SUSE Linux Enterprise Desktop possui um pacote básico com suporte genérico ao NetworkManager. Além disso, você também precisa instalar o respectivo pacote específico da área de trabalho para o seu applet.

OpenVPN

Para usar esta tecnologia VPN, instale

- `NetworkManager-openvpn` e
- `NetworkManager-openvpn-gnome`.

vpnc (Cisco)

Para usar esta tecnologia VPN, instale

- `NetworkManager-vpnc` e
- `NetworkManager-vpnc-gnome`.

PPTP (Point-to-Point Tunneling Protocol)

Para usar esta tecnologia VPN, instale

- `NetworkManager-pptp` e
- `NetworkManager-pptp-gnome`.

Após instalar os pacotes, configure sua conexão VPN conforme descrito no *Procedimento 22.1, "Adicionando e editando conexões"*.

22.4 NetworkManager e segurança

O NetworkManager distingue dois tipos de conexões wireless: confiáveis e não confiáveis. Uma conexão confiável é qualquer rede selecionada explicitamente no passado. Todas as outras são não confiáveis. As conexões confiáveis são identificadas pelo nome e pelo endereço MAC do ponto de acesso. O uso do endereço MAC garante que você não possa usar um ponto de acesso diferente com o nome da conexão confiável.

O NetworkManager faz uma exploração periódica de redes wireless disponíveis. Se forem encontradas várias redes confiáveis, a usada mais recentemente será selecionada automaticamente. O NetworkManager aguarda a sua seleção caso nenhuma das redes seja confiável.

Se a configuração de criptografia mudar, mas o nome e o endereço MAC continuarem os mesmos, o NetworkManager tentará se conectar, mas primeiro você será solicitado a confirmar as novas configurações de criptografia e fornecer atualizações, como uma nova chave.

Se você mudar da conexão wireless para o modo offline, o NetworkManager deixará o SSID ou o ESSID em branco. Isso garante que a placa seja desconectada.

22.4.1 Conexões de usuário e sistema

O NetworkManager conhece dois tipos de conexões: conexões de `usuário` e `sistema`. As conexões de usuário são aquelas que ficam disponíveis ao NetworkManager quando o primeiro usuário efetua login. Quaisquer credenciais necessárias são solicitadas ao usuário e, quando ele efetua logout, as conexões são desconectadas e removidas do NetworkManager. As conexões definidas como sendo de sistema podem ser compartilhadas por todos os usuários e disponibilizadas logo após o NetworkManager ser iniciado, antes que qualquer usuário efetue login. No caso das conexões do sistema, todas as credenciais devem ser fornecidas no momento em que a conexão é criada. Tais conexões do sistema podem ser usadas para conectar-se automaticamente a redes que exigem autorização. Para obter informações sobre como configurar conexões de usuário ou de sistema com o NetworkManager, consulte a *Seção 22.3, "Configurando conexões de rede"*.

22.4.2 Armazenando senhas e credenciais

Para não ter que digitar suas credenciais toda vez que se conectar a uma rede criptografada, você pode usar o Gerenciador de Chaveiros do GNOME para armazenar as credenciais criptografadas no disco, protegidas por uma senha master.

O NetworkManager também pode recuperar seus certificados para conexões seguras (por exemplo, conexões com fio, wireless ou VPN criptografadas) do armazenamento de certificado. Para obter mais informações, consulte o *Book "*Security Guide*" 12 "Certificate Store"*.

22.5 Perguntas mais frequentes

Veja a seguir algumas perguntas frequentes sobre a configuração de opções de rede especiais com o NetworkManager.

22.5.1 Como vincular uma conexão a um dispositivo específico?

Por padrão, as conexões no NetworkManager são específicas ao tipo de dispositivo: elas se aplicam a todos os dispositivos físicos do mesmo tipo. Se houver mais de um dispositivo físico disponível por tipo de conexão (por exemplo, quando a máquina está equipada com duas placas Ethernet), você poderá vincular uma conexão a determinado dispositivo.

Para fazer isso no GNOME, primeiro procure o endereço MAC do seu dispositivo (use as *Informações da Conexão* disponíveis no applet ou use a saída das ferramentas de linha de comando, como `nm-tool` ou `wicked show all`). Em seguida, inicie a caixa de diálogo para configurar conexões de rede e escolher a conexão que você deseja modificar. Na guia *Com fio* ou *Wireless*, digite o *Endereço MAC* do dispositivo e confirme suas mudanças.

22.5.2 Como especificar um determinado ponto de acesso caso sejam detectados vários pontos de acesso com o mesmo ESSID?

Quando há vários pontos de acesso disponíveis com bandas wireless diferentes (a/b/g/n), o ponto de acesso com o sinal mais forte é automaticamente escolhido por padrão. Para anular isso, use o campo *BSSID* ao configurar conexões wireless.

O BSSID (Basic Service Set Identifier) identifica de forma exclusiva cada Conjunto de Serviços Básicos. Em um Conjunto de Serviços Básicos de infraestrutura, o BSSID é o endereço MAC do ponto de acesso wireless. Em um Conjunto de Serviços Básicos independente (ad-hoc), o BSSID é um endereço MAC administrado localmente, gerado de um número aleatório de 46 bits.

Inicie a caixa de diálogo para configurar conexões de rede conforme descrito na *Seção 22.3, “Configurando conexões de rede”*. Escolha a conexão wireless que você deseja modificar e clique em *Editar*. Na guia *Wireless*, digite o BSSID.

22.5.3 Como compartilhar conexões de rede com outros computadores?

O dispositivo principal (que está conectado à Internet) não precisa de nenhuma configuração especial. Entretanto, você deve configurar o dispositivo que está conectado ao barramento local ou à máquina, conforme a seguir:

1. Inicie a caixa de diálogo para configurar conexões de rede conforme descrito na *Seção 22.3, “Configurando conexões de rede”*. Escolha a conexão que você deseja modificar e clique em *Editar*. Alterne para a guia *Configurações IPv4* e, na caixa

suspensa *Método*, escolha *Compartilhado com outros computadores*. Isso habilitará o encaminhamento de tráfego IP e executar um servidor DHCP no dispositivo. Confirme suas mudanças no NetworkManager.

2. Como o servidor DCHP utiliza a porta `67`, verifique se ela não está bloqueada pelo firewall: Na máquina que compartilha as conexões, inicie o YaST e selecione *Segurança e Usuários* › *Firewall*. Alterne para a categoria *Serviços Permitidos*. Se o *Servidor DCHP* ainda não for exibido como *Serviço Permitido*, selecione *Servidor DCHP* em *Serviços a Permitir* e clique em *Adicionar*. Confirme as mudanças no YaST.

22.5.4 Como fornecer informações de DNS estático com endereços automáticos (DHCP, PPP, VPN)?

Caso um servidor DHCP forneça informações (e/ou rotas) inválidas de DNS, você pode anulá-las. Inicie a caixa de diálogo para configurar conexões de rede conforme descrito na *Seção 22.3, "Configurando conexões de rede"*. Escolha a conexão que você deseja modificar e clique em *Editar*. Alterne para a guia *Configurações IPv4* e, na caixa suspensa *Método*, escolha *Somente endereços (DHCP) automáticos*. Digite as informações de DNS nos campos *Servidores DNS* e *Domínios de Pesquisa*. Para *Ignorar automaticamente rotas obtidas*, clique em *Rotas* e ative a respectiva caixa de seleção. Confirme as mudanças.

22.5.5 Como fazer o NetworkManager conectar-se a redes protegidas por senha antes que um usuário efetue login?

Defina uma `conexão do sistema` que possa ser usada para esse fim. Para obter mais informações, consulte a *Seção 22.4.1, "Conexões de usuário e sistema"*.

22.6 Solução de problemas

Podem ocorrer problemas de conexão. Alguns problemas comuns relacionados ao NetworkManager são: o applet não é iniciado ou opção ausente na VPN. Métodos para resolver e evitar esses problemas dependem da ferramenta usada.

O applet da área de trabalho do NetworkManager não é iniciado

Os applets serão iniciados automaticamente se a rede for configurada para controle do NetworkManager. Se o applet não for iniciado, verifique se o NetworkManager está habilitado no YaST, conforme descrito na *Seção 22.2, "Habilitando ou desabilitando o NetworkManager"*. Em seguida, verifique se o pacote NetworkManager-gnome também está instalado.

Se o applet da área de trabalho estiver instalado, mas não for executado por alguma razão, inicie-o manualmente. Se o applet de área de trabalho estiver instalado, mas não estiver em execução por algum motivo, inicie-o manualmente com o comando **`nm-applet`**.

O applet do NetworkManager não inclui a opção VPN

O suporte a NetworkManager, applets e VPN para NetworkManager é distribuído em pacotes separados. Se o applet NetworkManager não incluir a opção VPN, verifique se os pacotes com suporte ao NetworkManager referentes à sua tecnologia VPN estão instalados. Para obter mais informações, consulte a *Seção 22.3.4, "NetworkManager e VPN"*.

Nenhuma conexão de rede disponível

Se você configurou sua conexão de rede corretamente e todos os outros componentes para a conexão de rede (roteador etc.) também estiverem em funcionamento, pode ser útil reiniciar as interfaces de rede no seu computador. Para isso, efetue login em uma linha de comando como `root` e execute **`systemctl restart wicked.services`**.

22.7 Para obter mais informações

Você encontra mais informações sobre o NetworkManager nos seguintes sites na Web e diretórios:

Página do Projeto NetworkManager

http://projects.gnome.org/NetworkManager/

Documentação do pacote

Consulte também o conteúdo dos seguintes diretórios para obter as informações mais recentes sobre o NetworkManager e o applet do GNOME:

- `/usr/share/doc/packages/NetworkManager/`,
- `/usr/share/doc/packages/NetworkManager-gnome/`.

23 Samba

Com o Samba, uma máquina Unix pode ser configurada como um servidor de arquivos e de impressão para máquinas Mac OS X, Windows e OS/2. O Samba se tornou um produto completo e bastante complexo. Configure o Samba com o YaST ou editando o arquivo de configuração manualmente.

23.1 Terminologia

A seguir são apresentados alguns termos usados na documentação do Samba e no módulo YaST.

Protocolo SMB

O Samba usa o protocolo SMB (bloco de mensagens do servidor), que é baseado nos serviços NetBIOS. A Microsoft lançou o protocolo para que outros fabricantes de software pudessem estabelecer conexões com uma rede de domínio Microsoft. Com o Samba, o protocolo SMB opera acima do protocolo TCP/IP, de modo que este último precisa estar instalado em todos os clientes.

Protocolo CIFS

O protocolo CIFS (sistema de arquivos da Internet comuns) é outro protocolo que possui suporte no Samba. O CIFS é um protocolo de acesso padrão a sistemas de arquivos remotos para utilização pela rede, permitindo que grupos de usuários trabalhem juntos e compartilhem documentos pela rede.

NetBIOS

NetBIOS é uma interface de software (API) projetada para a comunicação entre máquinas que fornecem serviço de nomes. Ele permite que máquinas conectadas à rede reservem nomes para si. Após a reserva, essas máquinas podem ser tratadas pelo nome. Não há um processo central para a verificação de nomes. Qualquer máquina da rede pode reservar quantos nomes quiser, contanto que os nomes não estejam em uso ainda. A interface NetBIOS pode ser implementada para diferentes arquiteturas de rede. Uma implementação que funciona com relativa proximidade com o hardware da rede é chamada de NetBEUI, mas ela muitas vezes é chamada de NetBIOS. Os protocolos de rede implementados com o NetBIOS são o IPX da Novell (NetBIOS via TCP/IP) e TCP/IP.

Os nomes de NetBIOS enviados por TCP/IP não possuem nada em comum com os nomes usados em `/etc/hosts` ou com os nomes definidos pelo DNS. O NetBIOS usa sua própria convenção de nomes independente. Contudo, é recomendável usar nomes que correspondam aos nomes de host DNS para facilitar a administração ou usar o DNS nativamente. Esse é o padrão usado pelo Samba.

Servidor Samba

O servidor Samba fornece serviços SMB/CIFS e serviços de nomeação NetBIOS por IP aos clientes. Para o Linux, existem três daemons para servidor Samba: smbd para serviços SMB/CIFS, nmbd para serviços de nomeação e winbind para autenticação.

Cliente Samba

O cliente Samba é um sistema que usa serviços Samba de um servidor Samba pelo protocolo SMB. Todos os sistemas operacionais comuns, como Mac OS X, Windows e OS/2, prestam suporte ao protocolo SMB. O protocolo TCP/IP precisa estar instalado em todos os computadores. O Samba oferece um cliente para as diferentes versões do Unix. No caso do Linux, há um módulo de kernel para SMB que permite a integração de recursos SMB no nível de sistema Linux. Não é necessário executar nenhum daemon para o cliente Samba.

Compartilhamentos

Os servidores SMB oferecem recursos aos clientes por meio de compartilhamentos. Compartilhamentos são impressoras e diretórios com seus subdiretórios no servidor. Ele é exportado por meio de um nome e pode ser acessado pelo nome. O nome do compartilhamento pode ser definido como qualquer nome, não precisa ser o nome do diretório de exportação. Uma impressora também recebe um nome. Os clientes podem acessar a impressora pelo nome.

DC

Um controlador de domínio (DC) é um servidor que gerencia contas em um domínio. Para a replicação de dados, os controladores de domínio adicionais estão disponíveis em um domínio.

23.2 Instalando um servidor Samba

Para instalar um servidor Samba, inicie o YaST e selecione *Software* › *Gerenciamento de Software*. Escolha *Ver* › *Padrões* e selecione *Servidor de Arquivos*. Confirme a instalação dos pacotes necessários para concluir o processo de instalação.

23.3 Configurando um servidor Samba

Para configurar um servidor Samba, consulte a documentação do SUSE Linux Enterprise Server.

23.4 Configurando clientes

Os clientes somente podem acessar o servidor Samba via TCP/IP. O NetBEUI e o NetBIOS via IPX não podem ser usados com o Samba.

23.4.1 Configurando um cliente Samba com o YaST

Configure um cliente Samba para acessar recursos (arquivos ou impressoras) no servidor Samba ou Windows. Digite o domínio NT ou Active Directory ou o grupo de trabalho na caixa de diálogo *Serviços de Rede* › *Participação no Domínio do Windows*. Se você ativar *Também Usar Informação SMB para Autenticação Linux*, a autenticação do usuário será executada no servidor Samba, NT ou Kerberos.

Clique em *Configurações de Especialista* para ver as opções de configuração avançadas. Por exemplo, use a tabela *Montar Diretórios do Servidor* para habilitar a montagem de diretório pessoal do servidor automaticamente com autenticação. Assim os usuários poderão acessar seus diretórios pessoais quando estiverem hospedados no CIFS. Para ver os detalhes, consulte a página de manual de `pam_mount`.

Após concluir todas as configurações, confirme a caixa de diálogo para terminar a configuração.

23.5 Samba como servidor de login

Em redes onde se encontram predominantemente clientes Windows, muitas vezes é preferível que os usuários somente possam se registrar com uma conta e senha válidos. Em uma rede baseada no Windows, essa tarefa é gerenciada por um PDC (primary domain controller — controlador de domínio primário). Você pode usar um servidor Windows NT configurado como PDC, mas essa tarefa também pode ser executada com um servidor Samba. As entradas a serem feitas na seção `[global]` de `smb.conf` aparecem em *Exemplo 23.1, "Seção global em smb.conf"*.

EXEMPLO 23.1 SEÇÃO GLOBAL EM SMB.CONF

```
[global]
    workgroup = WORKGROUP
    domain logons = Yes
    domain master = Yes
```

É necessário preparar contas e senhas de usuários em formato de criptografia compatível com o Windows. Para isso, use o comando **smbpasswd -a name**. Crie a conta de domínio dos computadores, exigida pelo conceito de domínio do Windows , com os seguintes comandos:

```
useradd hostname\$
smbpasswd -a -m hostname
```

Com o comando **useradd**, um símbolo de cifrão é adicionado. O comando **smbpasswd** insere esse símbolo automaticamente quando o parâmetro `-m` é usado. O exemplo de configuração comentado (`/usr/share/doc/packages/samba/examples/smb.conf.SUSE`) contém configurações que automatizam essa tarefa.

```
add machine script = /usr/sbin/useradd -g nogroup -c "NT Machine Account" \
-s /bin/false %m\$
```

Para certificar-se de que o Samba possa executar esse script corretamente, escolha um usuário do Samba com as permissões de administrador necessárias e adicione-o ao grupo `ntadmin`. Em seguida, será possível atribuir a todos os usuários pertencentes a esse grupo Linux o status de `Domain Admin` com o comando:

```
net groupmap add ntgroup="Domain Admins" unixgroup=ntadmin
```

23.6 Tópicos avançados

Esta seção apresenta técnicas mais avançadas para gerenciar a parte tanto do cliente quanto do servidor da suíte do Samba.

23.6.1 Compactação de arquivos transparente no Btrfs

O Samba permite aos clientes manipular remotamente os flags de compactação de arquivos e diretórios para compartilhamentos localizados no sistema de arquivos Btrfs. O Windows Explorer oferece um recurso para marcar arquivos/diretórios para compactação transparente em *Arquivo* › *Propriedades* › *Avançado* caixa de diálogo:

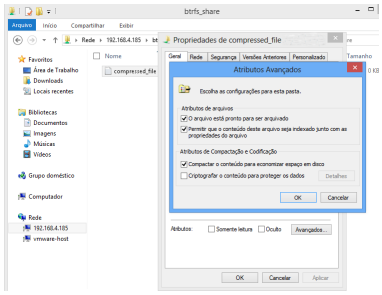

btrfs_share
Propriedades de compressed_file
Atributos Avançados
Escolha as configurações para esta pasta.
Atributos de arquivos
O arquivo está pronto para ser arquivado
Atributos de Compactação e Codificação
Compactar o conteúdo para economizar espaço em disco
Criptografar o conteúdo para proteger os dados
OK
Cancelar

FIGURA 23.1 CAIXA DE DIÁLOGO *ATRIBUTOS AVANÇADOS* DO WINDOWS EXPLORER

Os arquivos marcados para compactação são compactados de forma transparente e descompactados pelo sistema de arquivos base quando acessados ou modificados. Isso normalmente resulta em economia na capacidade de armazenamento em detrimento do overhead extra da CPU ao acessar o arquivo. Os arquivos e diretórios novos herdam o flag de compactação do diretório pai, exceto quando criados com a opção FILE_NO_COMPRESSION.

O Windows Explorer apresenta os arquivos e diretórios compactados de forma visualmente diferente daqueles não compactados:

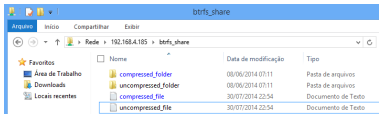


FIGURA 23.2 LISTAGEM DE DIRETÓRIOS DO WINDOWS EXPLORER COM ARQUIVOS COMPACTADOS

É possível habilitar a compactação de compartilhamentos Samba manualmente adicionando

```
vfs objects = btrfs
```

à configuração do compartilhamento em `/etc/samba/smb.conf` ou usando o YaST: *Serviços de Rede* › *Servidor Samba* › *Adicionar* e marcando *Utilizar Recursos do Btrfs*.

23.6.2 Instantâneos

Os instantâneos, também chamados de Cópias de Sombra, são cópias do estado do subvolume de um sistema de arquivos em determinado período. O Snapper é a ferramenta que gerencia os instantâneos no Linux. Os instantâneos são suportados no sistema de arquivos Btrfs ou em volumes LVM com aprovisionamento dinâmico. A suíte do Samba suporta o gerenciamento de instantâneos remotos por meio do protocolo FSRVP tanto no servidor quanto no cliente.

23.6.2.1 Versões anteriores

É possível expor os instantâneos do servidor Samba a clientes do Windows remotos como versões anteriores de arquivos ou diretórios.

Para habilitar instantâneos no servidor Samba, as seguintes condições devem ser atendidas:

- O compartilhamento de rede SMB reside em um subvolume Btrfs.
- O caminho do compartilhamento de rede SMB possui um arquivo de configuração do snapper relacionado. É possível criar o arquivo do snapper com

  ```
  snapper -c <cfg_name> create-config /path/to/share
  ```

  Para obter mais informações sobre o snapper, consulte o *Capítulo 4, Recuperação de sistema e gerenciamento de instantâneos com o Snapper*.
- A árvore do diretório do instantâneo deve permitir o acesso de usuários relevantes. Para obter mais informações, consulte a seção PERMISSIONS (Permissões) da página de manual de vfs_snapper (`man 8 vfs_snapper`).

Para suportar instantâneos remotos, é necessário modificar o arquivo `/etc/samba/smb.conf`. Você pode fazer isso com o *YaST*, em *Serviços de Rede* › *Servidor Samba*, ou manualmente, incrementando a seção do compartilhamento relevante com

```
vfs objects = snapper
```

Observe que é necessário reiniciar o serviço Samba para que as mudanças manuais em `smb.conf` entrem em vigor:

```
systemctl restart nmb.service smb.service
```

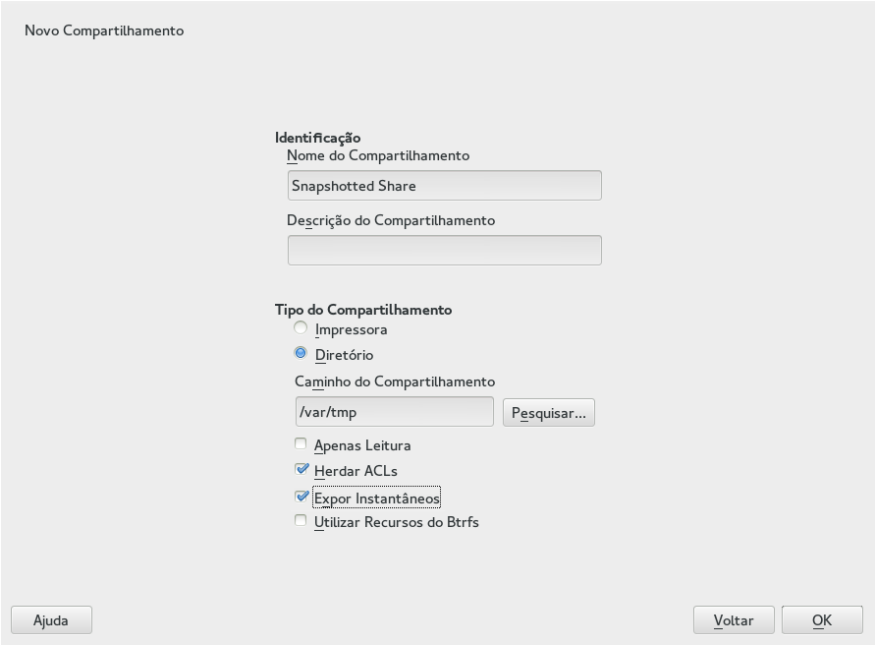


FIGURA 23.3 ADICIONANDO UM NOVO COMPARTILHAMENTO SAMBA COM CRIAÇÃO DE INSTANTÂNEO HABILITADA

Depois de configurados, os instantâneos criados pelo snapper para o caminho do compartilhamento Samba poderão ser acessados pelo Windows Explorer da guia *Versões Anteriores* de um arquivo ou diretório.

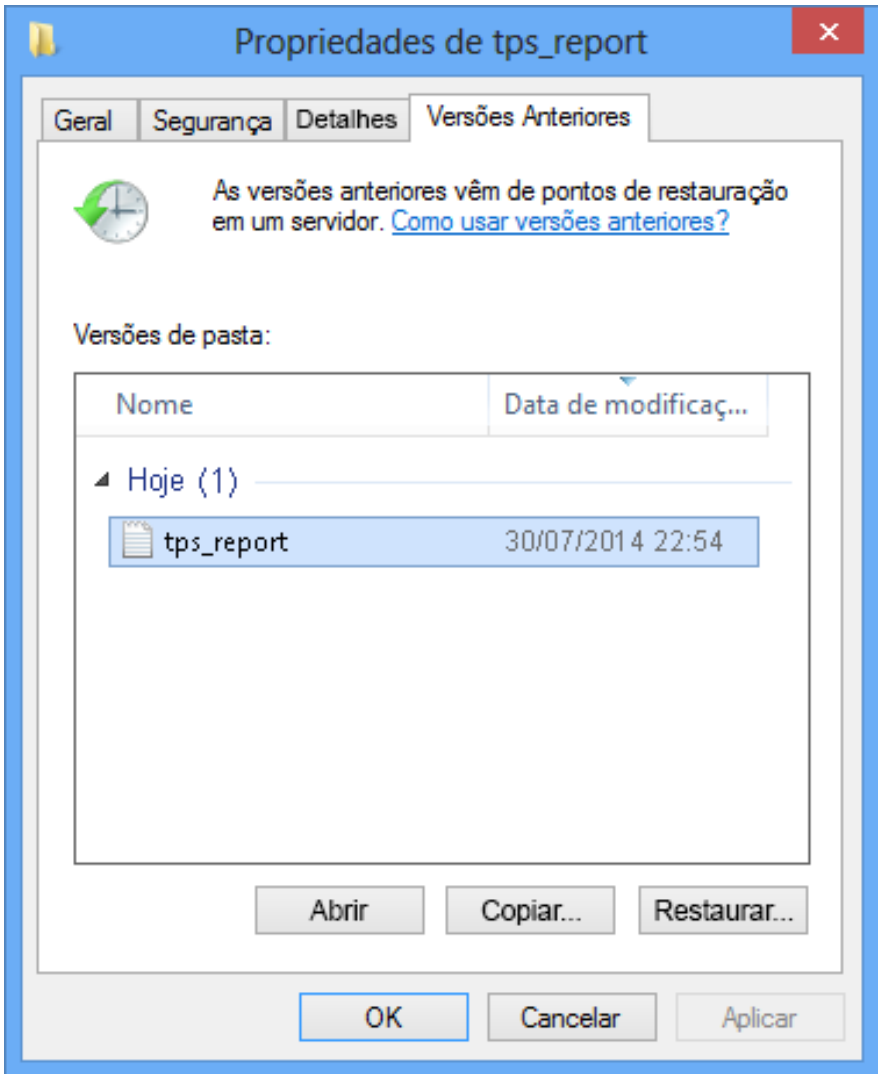


FIGURA 23.4 A GUIA *VERSÕES ANTERIORES* NO WINDOWS EXPLORER

23.6.2.2 Instantâneos de compartilhamentos remotos

Por padrão, só é possível criar e apagar instantâneos do servidor Samba localmente, pelo utilitário de linha de comando snapper ou usando o recurso de linha do tempo do snapper.

É possível configurar o Samba para processar solicitações de criação e exclusão de instantâneos do compartilhamento de hosts remotos usando o FSRVP (File Server Remote VSS Protocol – Protocolo VSS Remoto do Servidor de Arquivos).

Além da configuração e dos pré-requisitos documentados em *Seção 23.6.2.1, "Versões anteriores"*, a seguinte configuração global é necessária no `/etc/samba/smb.conf`:

```
[global]
rpc_daemon:fssd = fork
registry shares = yes
include = registry
```

Os clientes FSRVP, incluindo o **`rpcclient`** do Samba e o **`DiskShadow.exe`** do Windows Server 2012, podem instruir o Samba a criar ou apagar um instantâneo de determinado compartilhamento e o expor como um novo compartilhamento.

23.6.2.3 Gerenciando instantâneos do Linux remotamente com `rpcclient`

O pacote `samba-client` inclui o cliente FSRVP que pode solicitar remotamente a um servidor Windows/Samba para criar e expor um instantâneo de determinado compartilhamento. Em seguida, é possível usar as ferramentas existentes no SUSE Linux Enterprise Server para montar o compartilhamento exposto e fazer backup de seus arquivos. As solicitações ao servidor são enviadas usando o binário **`rpcclient`**.

EXEMPLO 23.2 USANDO O `rpcclient` PARA SOLICITAR INSTANTÂNEOS DE COMPARTILHAMENTO DO WINDOWS SERVER 2012

Conecte-se ao servidor `win-server.example.com` como administrador em um domínio `EXAMPLE`:

```
# rpcclient -U 'EXAMPLE\Administrator' ncacn_np:win-
server.example.com[ndr64,sign]
Enter EXAMPLE/Administrator's password:
```

Verifique se o compartilhamento SMB está visível para **`rpcclient`**:

```
rpcclient $> netshareenum
netname: windows_server_2012_share
remark:
path:   C:\Shares\windows_server_2012_share
```

```
password:       (null)
```

Verifique se o compartilhamento SMB suporta criação de instantâneo:

```
rpcclient $> fss_is_path_sup windows_server_2012_share \
UNC \\WIN-SERVER\windows_server_2012_share\ supports shadow copy requests
```

Solicite a criação de um instantâneo de compartilhamento:

```
rpcclient $> fss_create_expose backup ro windows_server_2012_share
13fe880e-e232-493d-87e9-402f21019fb6: shadow-copy set created
13fe880e-e232-493d-87e9-402f21019fb6(1c26544e-8251-445f-be89-d1e0a3938777): \
\\WIN-SERVER\windows_server_2012_share\ shadow-copy added to set
13fe880e-e232-493d-87e9-402f21019fb6: prepare completed in 0 secs
13fe880e-e232-493d-87e9-402f21019fb6: commit completed in 1 secs
13fe880e-e232-493d-87e9-402f21019fb6(1c26544e-8251-445f-be89-d1e0a3938777): \
share windows_server_2012_share@{1C26544E-8251-445F-BE89-D1E0A3938777} \
exposed as a snapshot of \\WIN-SERVER\windows_server_2012_share\
```

Confirme se o compartilhamento de instantâneo foi exposto pelo servidor:

```
rpcclient $> netshareenum
netname: windows_server_2012_share
remark:
path:   C:\Shares\windows_server_2012_share
password:       (null)

netname: windows_server_2012_share@{1C26544E-8251-445F-BE89-D1E0A3938777}
remark: (null)
path:   \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy{F6E6507E-F537-11E3-9404-
B8AC6F927453}\Shares\windows_server_2012_share\
password:       (null)
```

Tente apagar o compartilhamento de instantâneo:

```
rpcclient $> fss_delete windows_server_2012_share \
13fe880e-e232-493d-87e9-402f21019fb6 1c26544e-8251-445f-be89-d1e0a3938777
13fe880e-e232-493d-87e9-402f21019fb6(1c26544e-8251-445f-be89-d1e0a3938777): \
```

```
\\WIN-SERVER\windows_server_2012_share\ shadow-copy deleted
```

Confirme se o compartilhamento de instantâneo foi removido pelo servidor:

```
rpcclient $> netshareenum
netname: windows_server_2012_share
remark:
path:   C:\Shares\windows_server_2012_share
password:       (null)
```

23.6.2.4 Gerenciando instantâneos do Windows remotamente com `DiskShadow.exe`

É possível gerenciar instantâneos de compartilhamentos SMB no servidor Samba do Linux do ambiente Windows agindo também como cliente. O Windows Server 2012 inclui o utilitário **`DiskShadow.exe`**, que gerencia compartilhamentos remotos parecidos com o **`rpcclient`**, descrito em *Seção 23.6.2.3, "Gerenciando instantâneos do Linux remotamente com `rpcclient`"*. Observe que é necessário primeiro configurar o servidor Samba com atenção.

Veja a seguir um exemplo do procedimento de configuração do servidor Samba para que o cliente do Windows Server possa gerenciar os instantâneos de seu compartilhamento. Observe que EXAMPLE é o domínio Active Directory usado no ambiente de teste, fsrvp-server.example.com é o nome de host do servidor Samba e `/srv/smb` é o caminho para o compartilhamento SMB.

PROCEDIMENTO 23.1 CONFIGURAÇÃO DETALHADA DO SERVIDOR SAMBA

1. Entre no domínio Active Directory pelo YaST.
2. Verifique se a entrada DNS do Domínio Ativo estava correta:

```
fsrvp-server:~ # net -U 'Administrator' ads dns register \
fsrvp-server.example.com <IP address>
Successfully registered hostname with DNS
```

3. Criar subvolume Btrfs em `/srv/smb`

```
fsrvp-server:~ # btrfs subvolume create /srv/smb
```

4. Criar arquivo de configuração do snapper para o caminho `/srv/smb`

```
fsrvp-server:~ # snapper -c <snapper_config> create-config /srv/smb
```

5. Crie um novo compartilhamento com o caminho `/srv/smb` e a caixa de seleção *Expor Instantâneos* do YaST habilitada. Adicione os seguintes trechos à seção global do `/etc/samba/smb.conf`, como mencionado em *Seção 23.6.2.2, "Instantâneos de compartilhamentos remotos"*:

```
[global]
 rpc_daemon:fssd = fork
 registry shares = yes
 include = registry
```

6. Reiniciar o Samba com **`systemctl restart nmb.service smb.service`**

7. Configure permissões do snapper:

```
fsrvp-server:~ # snapper -c <snapper_config> set-config \
ALLOW_USERS="EXAMPLE\\\\Administrator EXAMPLE\\\\win-client$"
```

Verifique se todos ALLOW_USERS também têm permissão de passagem no subdiretório `.snapshots`.

```
fsrvp-server:~ # snapper -c <snapper_config> set-config SYNC_ACL=yes
```

Importante: Escape de caminho

Tenha cuidado com os escapes "\"! Inclua dois escapes para garantir que o valor armazenado em `/etc/snapper/configs/<config_snapper>` fique com apenas um escape.

"EXAMPLE\win-client$" corresponde à conta de computador cliente do Windows. O Windows emitirá as solicitações FSRVP iniciais enquanto estiver autenticado nessa conta.

8. Conceda os privilégios necessários para a conta de cliente do Windows:

```
fsrvp-server:~ # net -U 'Administrator' rpc rights grant \
"EXAMPLE\\win-client$" SeBackupPrivilege
```

```
Successfully granted rights.
```

O comando anterior não é necessário para o usuário "EXAMPLE\Administrator", que já recebeu os privilégios.

PROCEDIMENTO 23.2 CONFIGURAÇÃO DO CLIENTE DO WINDOWS E `DiskShadow.exe` EM AÇÃO

1. Inicialize o Windows Server 2012 (exemplo de nome de host WIN-CLIENT).
2. Entre no mesmo domínio Active Directory EXAMPLE do SUSE Linux Enterprise Server.
3. Reinicializar.
4. Abra o Powershell.
5. Inicie o **`DiskShadow.exe`** e comece o procedimento de backup:

```
PS C:\Users\Administrator.EXAMPLE> diskshadow.exe
Microsoft DiskShadow version 1.0
Copyright (C) 2012 Microsoft Corporation
On computer:  WIN-CLIENT,  6/17/2014 3:53:54 PM

DISKSHADOW> begin backup
```

6. Especifique para a cópia de sombra persistir após a saída, redefinição ou reinicialização do programa:

```
DISKSHADOW> set context PERSISTENT
```

7. Verifique se o compartilhamento especificado suporta instantâneos e crie um:

```
DISKSHADOW> add volume \\fsrvp-server\sles_snapper

DISKSHADOW> create
Alias VSS_SHADOW_1 for shadow ID {de4ddca4-4978-4805-8776-cdf82d190a4a} set as
 \
 environment variable.
Alias VSS_SHADOW_SET for shadow set ID {c58e1452-c554-400e-a266-d11d5c837cb1} \
 set as environment variable.
```

```
Querying all shadow copies with the shadow copy set ID \
 {c58e1452-c554-400e-a266-d11d5c837cb1}

 * Shadow copy ID = {de4ddca4-4978-4805-8776-cdf82d190a4a}     %VSS_SHADOW_1%
    - Shadow copy set: {c58e1452-c554-400e-a266-d11d5c837cb1}  %VSS_SHADOW_SET%
    - Original count of shadow copies = 1
    - Original volume name: \\FSRVP-SERVER\SLES_SNAPPER\ \
      [volume not on this machine]
    - Creation time: 6/17/2014 3:54:43 PM
    - Shadow copy device name:
      \\FSRVP-SERVER\SLES_SNAPPER@{31afd84a-44a7-41be-b9b0-751898756faa}
    - Originating machine: FSRVP-SERVER
    - Service machine: win-client.example.com
    - Not exposed
    - Provider ID: {89300202-3cec-4981-9171-19f59559e0f2}
    - Attributes:  No_Auto_Release Persistent FileShare

Number of shadow copies listed: 1
```

8. Conclua o procedimento de backup:

```
DISKSHADOW> end backup
```

9. Após criar o instantâneo, tente apagá-lo e confirme a exclusão:

```
DISKSHADOW> delete shadows volume \\FSRVP-SERVER\SLES_SNAPPER\
Deleting shadow copy {de4ddca4-4978-4805-8776-cdf82d190a4a} on volume \
 \\FSRVP-SERVER\SLES_SNAPPER\ from provider \
{89300202-3cec-4981-9171-19f59559e0f2} [Attributes: 0x04000009]...

Number of shadow copies deleted: 1

DISKSHADOW> list shadows all

Querying all shadow copies on the computer ...
No shadow copies found in system.
```

23.7 Para obter mais informações

A documentação do Samba acompanha o pacote `samba-doc`, que não é instalado por padrão. Instale-o com **`zypper install samba-doc`**. Digite **`apropos`** `samba` na linha de comando para exibir algumas páginas de manual ou procure por mais documentações e exemplos online no diretório `/usr/share/doc/packages/samba`. Encontre uma configuração de exemplo comentada (`smb.conf.SUSE`) no subdiretório `examples`. O outro arquivo no qual procurar informações relacionadas ao Samba é `/usr/share/doc/packages/samba/README.SUSE`.

O HOWTO do Samba (consulte https://wiki.samba.org), fornecido pela equipe Samba, inclui uma seção sobre solução de problemas. Além disso, a Parte V do documento oferece um guia passo a passo para a verificação da configuração.

24 Compartilhando sistemas de arquivos com o NFS

Distribuir e compartilhar sistemas de arquivos em uma rede é uma tarefa comum em ambientes corporativos. O reconhecido sistema de arquivos de rede (*NFS*) funciona com o *NIS*, o protocolo de yellow pages. Para um protocolo mais seguro que funcione com o *LDAP* e também possa usar Kerberos, marque *NFSv4*. Juntamente com o pNFS, é possível eliminar gargalos no desempenho.

O NFS com o NIS torna uma rede transparente para o usuário. Com o NFS, é possível distribuir sistemas de arquivos arbitrários pela rede. Com a configuração adequada, os usuários sempre ficam no mesmo ambiente, independentemente do terminal que estejam usando.

24.1 Terminologia

Veja a seguir os termos usados no módulo do YaST.

Exportações

Um diretório *exportado* por um servidor NFS, que os clientes podem integrar a seus sistemas.

Cliente NFS

O cliente NFS é um sistema que usa serviços NFS de um servidor NFS pelo protocolo NFS (Network File System – Sistema de Rede de Arquivos). O protocolo TCP/IP já está integrado ao kernel do Linux; não há necessidade de instalar software adicional.

Servidor NFS

O servidor NFS fornece serviços NFS aos clientes. Um servidor em execução depende dos seguintes daemons: `nfsd` (worker), `idmapd` (mapeamentos de nome de grupo e usuário para IDs e vice versa), `statd` (bloqueio de arquivos) e `mountd` (solicitações de montagem).

NFSv3

NFSv3 é a implementação da versão 3, o “antigo” NFS sem informações de estado que suporta autenticação do cliente.

NFSv4

NFSv4 é a nova implementação da versão 4 que suporta autenticação do usuário segura pelo kerberos. O NFSv4 requer uma única porta e, portanto, é mais adequado para ambientes protegidos por firewall do que o NFSv3.
O protocolo é especificado como http://tools.ietf.org/html/rfc3530.

pNFS

NFS Paralelo, o protocolo de extensão do NFSv4. Qualquer cliente do pNFS pode acessar diretamente os dados em um servidor NFS.

24.2 Instalando o servidor NFS

Para instalar e configurar um servidor NFS, consulte a documentação do SUSE Linux Enterprise Server.

24.3 Configurando clientes

Para configurar seu host como cliente NFS, você não precisa instalar software adicional. Todos os pacotes necessários são instalados por padrão.

24.3.1 Importando sistemas de arquivos com o YaST

Usuários autorizados podem montar diretórios NFS de um servidor NFS na árvore de arquivos local usando o módulo de cliente NFS do YaST. Proceda da seguinte maneira:

PROCEDIMENTO 24.1 IMPORTANDO DIRETÓRIOS NFS

1. Inicie o módulo de cliente NFS do YaST.
2. Clique em *Adicionar* na guia *Compartilhamentos NFS*. Digite o nome de host do servidor NFS, o diretório a ser importado e o ponto de montagem desse diretório localmente.
3. Ao usar o NFSv4, selecione *Habilitar NFSv4* na guia *Configurações do NFS*. O *Nome de Domínio NFSv4* também deve incluir o mesmo valor usado pelo servidor NFSv4. O domínio padrão é `localdomain`.

4. Para usar a autenticação Kerberos para o NFS, é preciso que a segurança GSS esteja habilitada. Selecione *Habilitar Segurança GSS*.

5. Habilite *Abrir Porta no Firewall* na guia *Configurações do NFS*, se você usa um Firewall e deseja permitir o acesso de computadores remotos ao serviço. O status do firewall é mostrado próximo à caixa de seleção.

6. Clique em *OK* para gravar as mudanças.

A configuração é gravada em `/etc/fstab` e os sistemas de arquivos especificados são montados. Quando você iniciar o cliente de configuração do YaST posteriormente, ele também lerá a configuração existente desse arquivo.

24.3.2 Importando sistemas de arquivos manualmente

O pré-requisito para importar os sistemas de arquivos manualmente de um servidor NFS é um mapeador de portas RPC em execução. O `nfs.service` toma cuidado para iniciá-lo apropriadamente; portanto, digite **`systemctl start nfs.service`** como `root` para iniciá-lo. Em seguida, os sistemas de arquivos remotos podem ser montados no sistema de arquivos como partições locais usando **`mount`**:

```
mount host:remote-pathlocal-path
```

Para importar os diretórios de usuário da máquina do `nfs.example.com`, por exemplo, use:

```
mount nfs.example.com:/home /home
```

24.3.2.1 Usando o serviço de montagem automática

O daemon autofs pode ser usado para montar sistemas de arquivos remotos automaticamente. Adicione a seguinte entrada ao seu arquivo `/etc/auto.master`:

```
/nfsmounts /etc/auto.nfs
```

Agora, o diretório `/nfsmounts` atuará como raiz para todas as montagens NFS no cliente se o arquivo `auto.nfs` for preenchido adequadamente. O nome `auto.nfs` foi escolhido por mera conveniência, você pode escolher qualquer nome. Adicione entradas ao `auto.nfs` para todas as montagens NFS da seguinte maneira:

```
localdata -fstype=nfs server1:/data
nfs4mount -fstype=nfs4 server2:/
```

Ative as configurações com **`systemctl start autofs.service`** como `root`. Neste exemplo, `/nfsmounts/localdata`, o diretório `/data` do `server1`, é montado com NFS e `/nfsmounts/nfs4mount`, do `server2`, é montado com NFSv4.

Se o arquivo `/etc/auto.master` for editado enquanto o serviço autofs estiver em execução, o automounter deverá ser reiniciado com **`systemctl restart autofs.service`** para as mudanças entrarem em vigor.

24.3.2.2 Editando `/etc/fstab` manualmente

Uma entrada de montagem típica do NFSv3 em `/etc/fstab` tem aparência semelhante a esta:

```
nfs.example.com:/data /local/path nfs rw,noauto 0 0
```

Para montagens do NFSv4, use `nfs4` em vez de `nfs` na terceira coluna:

```
nfs.example.com:/data /local/pathv4 nfs4 rw,noauto 0 0
```

A opção `noauto` impede que o sistema de arquivos seja montado automaticamente na inicialização. Se desejar montar o respectivo sistema de arquivos manualmente, é possível abreviar o comando de montagem especificando apenas o ponto de montagem:

```
mount /local/path
```

Nota

Se você não digitar a opção `noauto`, os scripts init do sistema gerenciarão a montagem dos sistemas de arquivos na inicialização.

24.3.3 NFS paralelo (pNFS)

NFS é um dos protocolos mais antigos, desenvolvido nos anos 80. Em geral, o NFS é suficiente para compartilhar arquivos pequenos. Entretanto, para transferir arquivos grandes ou quando um número elevado de clientes precisa acessar os dados, o servidor NFS torna-se um gargalo e afeta significativamente o desempenho do sistema. Isso ocorre porque os arquivos aumentam de tamanho rapidamente, mas a velocidade relativa da Ethernet não consegue acompanhar esse aumento.

Quando você solicita um arquivo de um servidor NFS "normal", o servidor procura os metadados do arquivo, coleta todos os dados e os transfere pela rede até o cliente. No entanto, o gargalo no desempenho torna-se aparente independentemente do tamanho dos arquivos:

- Com os arquivos pequenos, a maior parte do tempo é gasta para coletar os metadados.
- Com os arquivos grandes, a maior parte do tempo é gasta para transferir os dados do servidor para o cliente.

O pNFS, ou NFS paralelo, supera essa limitação, pois ele separa os metadados do sistema de arquivos do local dos dados. Para isso, o pNFS requer dois tipos de servidores:

- Um *servidor de controle* ou de *metadados* que controla todo o tráfego que não seja de dados
- Um ou mais *servidores de armazenamento* para armazenar os dados

Os servidores de metadados e de armazenamento formam um único servidor NFS lógico. Para o cliente ler ou gravar, o servidor de metadados informa ao cliente NFSv4 qual servidor de armazenamento deve ser usado para acessar os pacotes de arquivos. O cliente pode acessar os dados diretamente no servidor.

O SUSE Linux Enterprise suporta pNFS apenas no cliente.

24.3.3.1 Configurando o cliente pNFS com o YaST

Siga a descrição no *Procedimento 24.1, "Importando diretórios NFS"*, mas clique na caixa de seleção *pNFS (v4.1)* e, opcionalmente, em *Compartilhamento NFSv4*. O YaST executa todas as etapas necessárias e grava todas as opções exigidas no arquivo `/etc/exports`.

24.3.3.2 Configurando o cliente pNFS manualmente

Para começar, consulte a *Seção 24.3.2, "Importando sistemas de arquivos manualmente"*. A maior parte da configuração é feita pelo servidor NFSv4. Para o pNFS, a única diferença é adicionar a opção `minorversion` e o servidor de metadados *`MDS_SERVER`* ao comando **`mount`**:

```
mount -t nfs4 -o minorversion=1 MDS_SERVER MOUNTPOINT
```

Para ajudar na depuração, mude o valor no sistema de arquivos `/proc`:

```
echo 32767 > /proc/sys/sunrpc/nfsd_debug
echo 32767 > /proc/sys/sunrpc/nfs_debug
```

24.4 Para obter mais informações

Além das páginas de manual de **`exports`**, **`nfs`** e **`mount`**, há informações disponíveis sobre como configurar servidores e clientes NFS em `/usr/share/doc/packages/nfsidmap/README`. Para mais documentações online, consulte os seguintes sites na Web:

- A documentação técnica online encontra-se no SourceForge (http://nfs.sourceforge.net/).
- Para obter instruções sobre como configurar o NFS que usa Kerberos, consulte o documento NFS Version 4 Open Source Reference Implementation (http://www.citi.umich.edu/projects/nfsv4/linux/krb5-setup.html) (Implementação da referência de código-fonte aberto do NFSv4).
- Se você tiver dúvidas sobre o NFSv4, consulte as Perguntas frequentes do Linux NFSv4 (http://www.citi.umich.edu/projects/nfsv4/linux/faq/).

25 Montagem sob demanda com o Autofs

O `autofs` é um programa que monta automaticamente diretórios especificados sob demanda. Ele se baseia em um módulo do kernel para alta eficiência e pode gerenciar diretórios locais e compartilhamentos de rede. Estes pontos de montagem automática só são montados quando acessados e desmontados após um período de inatividade. Este comportamento sob demanda economiza largura de banda e promove um melhor desempenho do que as montagens estáticas gerenciadas por `/etc/fstab`. Enquanto o `autofs` é um script de controle, o **`automount`** é o comando (daemon) que faz a montagem automática propriamente dita.

25.1 Instalação

O `autofs` não é instalado no SUSE Linux Enterprise Desktop por padrão. Para usar seus recursos de montagem automática, instale-o primeiro com

```
sudo zypper install autofs
```

25.2 Configuração

Você deve configurar o `autofs` manualmente editando seus arquivos de configuração com um editor de texto, como o **`vim`**. Há duas etapas básicas para configurar o `autofs`: o arquivo de mapa *master* e os arquivos de mapa específicos.

25.2.1 O arquivo de mapa master

O arquivo de configuração master padrão do `autofs` é `/etc/auto.master`. É possível mudar seu local modificando o valor da opção `DEFAULT_MASTER_MAP_NAME` em `/etc/sysconfig/autofs`. Veja a seguir o conteúdo do padrão para o SUSE Linux Enterprise Desktop:

```
#
# Sample auto.master file
# This is an automounter map and it has the following format
# key [ -mount-options-separated-by-comma ] location
# For details of the format look at autofs(5).
```

```
#
#/misc  /etc/auto.misc ❷
#/net -hosts
#
# Include /etc/auto.master.d/*.autofs ❸
#
#+dir:/etc/auto.master.d
#
# Include central master map if it can be found using
# nsswitch sources.
#
# Note that if there are entries for /net or /misc (as
# above) in the included master map any keys that are the
# same will not be seen as the first read key seen takes
# precedence.
#
+auto.master ❹
```

❶ A página de manual do `autofs` (**`man 5 autofs`**) oferece muitas informações úteis sobre o formato dos mapas do automounter.

❷ Embora comentado (#) por padrão, esse é um exemplo de sintaxe de mapeamento simples do automounter.

❸ Caso seja necessário dividir o mapa master em vários arquivos, remova o comentário da linha e insira os mapeamentos (com o sufixo `.autofs`) no diretório `/etc/auto.master.d/`.

❹ `+auto.master` garante que os que usam o NIS ainda localizem o mapa master.

As entradas no `auto.master` possuem três campos com a seguinte sintaxe:

```
mount point      map name      options
```

mount point

O local base para montar o sistema de arquivos do `autofs`, como `/home`.

map name

O nome da origem do mapa para usar na montagem. Para ver a sintaxe dos arquivos de mapa, consulte a *Seção 25.2.2, "Arquivos de mapa"*.

opções

Estas opções (se especificadas) serão aplicadas como padrão a todas as entradas no mapa determinado.

Dica

Para obter informações mais detalhadas sobre os valores específicos do `map-type`, `format` e `options` opcional, consulte a página de manual do *auto.master* (**`man 5 auto.master`**).

A seguinte entrada no `auto.master` instrui o `autofs` a procurar em `/etc/auto.smb` e criar pontos de montagem no diretório `/smb`.

```
/smb   /etc/auto.smb
```

25.2.1.1 Montagens diretas

As montagens diretas criam um ponto de montagem no caminho especificado dentro do arquivo de mapa relevante. Em vez de especificar o ponto de montagem em `auto.master`, substitua o campo do ponto de montagem por `/-`. Por exemplo, a seguinte linha instrui o `autofs` a criar um ponto de montagem no local especificado em `auto.smb`:

```
/-        /etc/auto.smb
```

Dica: Mapas sem o caminho completo

Se o arquivo de mapa não for especificado com seu local completo ou caminho de rede, ele será localizado usando a configuração NSS (Name Service Switch):

```
/-        auto.smb
```

25.2.2 Arquivos de mapa

Importante: Outros tipos de mapas

Embora os *arquivos* sejam os tipos de mapas mais comuns para montagem automática com o `autofs`, existem também outros tipos. Uma especificação de mapa pode ser a saída de um comando ou o resultado de uma consulta no LDAP ou banco de dados. Para obter informações mais detalhadas sobre os tipos de mapas, consulte a página de manual `man 5 auto.master`.

Os arquivos de mapa especificam o local de origem (local ou rede) e o ponto de montagem no qual montar a origem localmente. O formato geral dos mapas é parecido com o mapa master. A diferença é que as *opções* aparecem entre o ponto de montagem e o local, e não no final da entrada:

```
mount point      options      location
```

mount point

Especifica onde montar o local de origem. Pode ser o nome de um diretório único (a chamada montagem *indireta*) a ser adicionado ao ponto de montagem base especificado em `auto.master` ou o caminho completo do ponto de montagem (montagem direta, consulte a *Seção 25.2.1.1, "Montagens diretas"*).

opções

Especifica a lista de opções de montagem separadas por vírgulas referentes às entradas relevantes. Se `auto.master` também incluir opções para este arquivo de mapa, elas serão anexadas.

location

Especifica o local de onde o sistema de arquivos deverá ser montado. Normalmente, trata-se de um volume NFS ou SMB na notação usual `host_name:path_name`. Se o sistema de arquivos a ser montado começar com uma "/" (como as entradas locais `/dev` ou os compartilhamentos smbfs), será necessário incluir um prefixo de dois-pontos ":", como `:/dev/sda1`.

25.3 Operação e depuração

Esta seção apresenta informações sobre como controlar a operação do serviço `autofs` e como ver mais informações sobre depuração ao ajustar a operação do automounter.

25.3.1 Controlando o serviço `autofs`

A operação do serviço `autofs` é controlada pelo `systemd`. A sintaxe geral do comando **`systemctl`** do `autofs` é

```
sudo systemctl sub-command autofs.service
```

em que o *`subcomando`* é um dos seguintes:

habilitar
: Inicia o daemon automounter na inicialização.

iniciar
: Inicia o daemon automounter.

parar
: Para o daemon automounter. Os pontos de montagem automática não estão acessíveis.

status
: Imprime o status atual do serviço `autofs` juntamente com a parte de um arquivo de registro relevante.

restart
: Para e inicia o automounter, terminando todos os daemons em execução e iniciando novos daemons.

reload
: Verifica o mapa `auto.master` atual, reinicia os daemons que tiveram suas entradas modificadas e inicia daemons novos para entradas novas.

25.3.2 Depurando problemas do automounter

Se você tiver algum problema para montar diretórios com o `autofs`, convém executar o daemon **`automount`** manualmente e observar as mensagens de saída:

1. Pare o `autofs`.

   ```
   sudo systemctl stop autofs.service
   ```

2. De um terminal, execute o **`automount`** manualmente em primeiro plano, gerando a saída verbosa.

   ```
   sudo automount -f -v
   ```

3. De outro terminal, tente montar os sistemas de arquivos de montagem automática acessando os pontos de montagem (por exemplo, por **`cd`** ou **`ls`**).

4. Verifique a saída do **`automount`** do primeiro terminal para obter mais informações sobre a falha na montagem ou porque não houve nenhuma tentativa.

25.4 Montando automaticamente um compartilhamento NFS

O procedimento a seguir ilustra como configurar o `autofs` para montar automaticamente um compartilhamento NFS disponível na rede. Ele usa as informações mencionadas anteriormente e assume que você esteja familiarizado com as exportações NFS. Para obter mais informações sobre NFS, consulte o *Capítulo 24, Compartilhando sistemas de arquivos com o NFS*.

1. Edite o arquivo de mapa master `/etc/auto.master`:

   ```
   sudo vim /etc/auto.master
   ```

   Adicione uma nova entrada para a nova montagem NFS ao final de `/etc/auto.master`:

   ```
   /nfs      /etc/auto.nfs      --timeout=10
   ```

   Ela informa ao `autofs` que o ponto de montagem base é `/nfs`, os compartilhamentos NFS estão especificados no mapa `/etc/auto.nfs` e todos os compartilhamentos nesse mapa serão automaticamente desmontados após 10 segundos de inatividade.

2. Crie um novo arquivo de mapa para os compartilhamentos NFS:

   ```
   sudo vim /etc/auto.nfs
   ```

Normalmente, o `/etc/auto.nfs` inclui uma linha separada para cada compartilhamento NFS. Seu formato está descrito na *Seção 25.2.2, "Arquivos de mapa"*. Adicione a linha que descreve o ponto de montagem e o endereço de rede do compartilhamento NFS:

```
export      jupiter.com:/home/geeko/doc/export
```

A linha acima indica que o diretório `/home/geeko/doc/export` no host `jupiter.com` será montado automaticamente no diretório `/nfs/export` no host local (`/nfs` é tirado do mapa `auto.master`) quando solicitado. O diretório `/nfs/export` será criado automaticamente pelo `autofs`.

3. Se preferir, comente a linha relacionada em `/etc/fstab` caso já tenha montado o mesmo compartilhamento NFS estaticamente. A linha deve ser parecida com o seguinte:

```
#jupiter.com:/home/geeko/doc/export /nfs/export nfs defaults 0 0
```

4. Recarregue o `autofs` e verifique se está funcionando:

```
sudo systemctl restart autofs.service
```

```
# ls -l /nfs/export
total 20
drwxr-xr-x  6 1001 users 4096 Oct 25 08:56 ./
drwxr-xr-x  3 root root     0 Apr  1 09:47 ../
drwxr-xr-x  5 1001 users 4096 Jan 14  2013 .images/
drwxr-xr-x 10 1001 users 4096 Aug 16  2013 .profiled/
drwxr-xr-x  3 1001 users 4096 Aug 30  2013 .tmp/
drwxr-xr-x  4 1001 users 4096 Oct 25 08:56 SLE-12-manual/
```

Se você conseguir ver a lista de arquivos no compartilhamento remoto, o `autofs` estará funcionando.

25.5 Tópicos avançados

Esta seção descreve os tópicos que vão além da introdução básica sobre o `autofs`: montagem automática dos compartilhamentos NFS disponíveis na sua rede, uso de curingas em arquivos de mapa e informações específicas do sistema de arquivos CIFS.

25.5.1 Ponto de montagem `/net`

Este ponto de montagem ajudante é útil quando você usa muitos compartilhamentos NFS. O `/net` monta automaticamente todos os compartilhamentos NFS na rede local sob demanda. A entrada já está presente no arquivo `auto.master`, portanto, tudo o que você precisa fazer é remover o comentário dela e reiniciar o `autofs`:

```
/net      -hosts
```

```
systemctl restart autofs.service
```

Por exemplo, se você tem um servidor chamado `jupiter` com um compartilhamento NFS denominado `/export`, pode montá-lo digitando

```
# cd /net/jupiter/export
```

na linha de comando.

25.5.2 Usando curingas para montar subdiretórios automaticamente

Se você tem um diretório com subdiretórios que precisa montar um a um automaticamente (a situação mais comum é o diretório `/home` com subdiretórios pessoais de usuários individuais), o `autofs` tem a solução ideal para você.

No caso de diretórios pessoais, adicione a seguinte linha em `auto.master`:

```
/home      /etc/auto.home
```

Será necessário adicionar o mapeamento correto ao arquivo `/etc/auto.home` para que os diretórios pessoais dos usuários sejam montados automaticamente. Uma solução é criar entradas separadas para cada diretório:

```
wilber      jupiter.com:/home/wilber
penguin      jupiter.com:/home/penguin
tux      jupiter.com:/home/tux
[...]
```

Isso é bastante incomum, já que você precisa gerenciar a lista de usuários dentro de `auto.home`. É possível usar o asterisco "*" no lugar do ponto de montagem e o E comercial "&" no lugar do diretório a ser montado:

```
*      jupiter:/home/&
```

25.5.3 Montando automaticamente o sistema de arquivos CIFS

Para montar automaticamente um compartilhamento SMB/CIFS (consulte o *Capítulo 23, Samba* para obter mais informações sobre o protocolo SMB/CIFS), é necessário modificar a sintaxe do arquivo de mapa. Adicione `-fstype=cifs` no campo de opção e inclua um prefixo de ":" no local do compartilhamento.

```
mount point      -fstype=cifs      ://jupiter.com/export
```

26 Sincronização de arquivos

Atualmente, muitas pessoas usam vários computadores: um em casa, um ou mais computadores no local de trabalho e possivelmente um laptop, tablet ou smartphone em trânsito. Vários arquivos são necessários em todos esses computadores. Talvez você queira trabalhar com todos os computadores e modificar os arquivos, de modo que a versão mais recente dos dados fique disponível em todos os computadores.

26.1 Software de sincronização de dados disponível

A sincronização de dados não é um problema para computadores permanentemente conectados por uma rede rápida. Nesse caso, use um sistema de arquivos de rede, como o NFS, e armazene os arquivos em um servidor para que todos os hosts acessem os mesmos dados via rede. Essa abordagem será impossível se a conexão de rede for instável ou não permanente. Quando você viaja com um laptop, precisa ter cópias de todos os arquivos necessários no disco rígido local. Entretanto, é necessário sincronizar os arquivos modificados. Quando você modificar um arquivo em um computador, verifique se uma cópia dele foi atualizada em todos os outros computadores. No caso de cópias ocasionais, elas podem ser feitas manualmente com o scp ou o rsync. Entretanto, se vários arquivos forem envolvidos, o procedimento poderá ser complicado e demandar muito cuidado para evitar erros, como a sobregravação de um arquivo novo por um antigo.

Atenção: risco de perda de dados

Antes de começar a gerenciar seus dados com um sistema de sincronização, você deve se informar sobre o programa usado e testar sua funcionalidade. É indispensável ter um backup de arquivos importantes.

A tarefa prolongada e sujeita a erros de sincronizar dados manualmente pode ser evitada se você usar um dos programas que utilizam vários métodos para automatizá-la. Os resumos a seguir têm o simples objetivo de dar uma visão geral sobre como esses programas funcionam e como podem ser usados. Se você planeja usá-los, leia a documentação do programa.

26.1.1 CVS

O CVS, que é mais usado para gerenciar versões de origem de programas, oferece a possibilidade de manter cópias dos arquivos em vários computadores. Dessa forma, ele também é adequado para sincronização de dados. O CVS mantém um repositório central no servidor, no qual os arquivos e as mudanças feitas neles são gravados. As mudanças realizadas localmente são enviadas para o repositório e podem ser recuperadas de outros computadores por meio de uma atualização. Todos os procedimentos devem ser iniciados pelo usuário.

O CVS é muito suscetível a erros quando ocorrem mudanças em vários computadores. As mudanças são fundidas e, se ocorrerem nas mesmas linhas, um conflito será reportado. Quando ocorre um conflito, o banco de dados permanece em estado consistente. O conflito só fica visível para resolução no host cliente.

26.1.2 rsync

Quando o controle de versão não é necessário, mas grandes estruturas de diretório precisam ser sincronizadas em conexões de rede lentas, a ferramenta rsync oferece mecanismos avançados para a transmissão apenas de mudanças entre arquivos. Isso não diz se aplica apenas a arquivos de texto, mas também a arquivos binários. Para detectar as diferenças entre os arquivos, o rsync os subdivide em blocos e calcula seus checksums.

O esforço dedicado à detecção das mudanças tem um preço. Os sistemas a serem sincronizados devem ser dimensionados generosamente para uso do rsync. A RAM é especialmente importante.

26.2 Determinando fatores para selecionar um programa

Há alguns fatores importantes a serem considerados ao decidir que programa será usado.

26.2.1 Cliente/Servidor X não hierarquia

Dois modelos diferentes são comumente usados para distribuir dados. No primeiro modelo, todos os clientes sincronizam seus arquivos com um servidor central. O servidor deve ser acessível a todos os clientes pelo menos ocasionalmente. Esse modelo é usado pelo CVS.

A outra possibilidade é deixar todos os hosts ligados em rede sincronizarem seus dados entre os pontos uns dos outros. O rsync funciona de fato no modo cliente, mas qualquer cliente também pode atuar como servidor.

26.2.2 Portabilidade

O CVS e o rsync também estão disponíveis para muitos outros sistemas operacionais, incluindo vários sistemas Unix e Windows.

26.2.3 Interativo versus automático

No CVS, a sincronização de dados começa manualmente pelo usuário. Isso permite um controle fino dos dados a serem sincronizados e um fácil gerenciamento de conflitos. No entanto, se os intervalos de sincronização forem muito longos, será mais provável que ocorram conflitos.

26.2.4 Conflitos: incidência e solução

Conflitos só ocorrem raramente no CVS, mesmo quando há muitas pessoas trabalhando em um grande projeto de programa. Isso ocorre porque os documentos são fundidos na base de linhas individuais. Quando ocorre um conflito, somente um cliente é afetado. Normalmente, os conflitos no CVS podem ser facilmente resolvidos.

Não há gerenciamento de conflitos no rsync. O usuário é responsável por não sobregravar acidentalmente arquivos e resolver manualmente todos os possíveis conflitos. Para fins de segurança, é possível empregar adicionalmente um sistema de controle de versão como o RCS.

26.2.5 Selecionando e adicionando arquivos

No CVS, diretórios e arquivos novos devem ser adicionados explicitamente com o comando `cvs add`. Esse procedimento resulta em um maior controle do usuário sobre os arquivos a serem sincronizados. Por outro lado, os arquivos novos quase sempre são despercebidos, principalmente quando os pontos de interrogação na saída de `cvs update` são ignorados por causa do grande número de arquivos.

26.2.6 Histórico

Um recurso adicional do CVS é a possibilidade de reconstrução de versões antigas de arquivos. Um breve comentário de edição pode ser inserido em cada mudança, e o desenvolvimento dos arquivos pode ser facilmente rastreado posteriormente com base no conteúdo dos comentários. Essa é uma ajuda valiosa para textos de teses e de programas.

26.2.7 Volume de dados e requisitos do disco rígido

Os discos rígidos de todos os hosts envolvidos devem ter espaço em disco suficiente para todos os dados distribuídos. O CVS requer espaço adicional para o banco de dados de repositório no servidor. O histórico do arquivo também é armazenado no servidor, requerendo ainda mais espaço. Quando arquivos em formato de texto são mudados, somente as linhas modificadas são gravadas. Arquivos binários requerem espaço em disco adicional relativo ao tamanho do arquivo sempre que ele for mudado.

26.2.8 GUI

Usuários experientes normalmente executam o CVS a partir da linha de comando. Entretanto, há interfaces gráficas do usuário disponíveis para Linux (como a cervisia) e para outros sistemas operacionais (como a wincvs). Muitas ferramentas de desenvolvimento e editores de texto (como o Emacs) oferecem suporte a CVS. É sempre mais fácil realizar a resolução de conflitos com esses front ends.

26.2.9 Facilidade de uso

O rsync é bastante fácil de usar, sendo também adequado para principiantes. O CVS é um pouco mais difícil de operar. Os usuários devem entender a interação entre o repositório e os dados locais. As mudanças dos dados devem ser primeiro fundidas localmente no repositório. Esse procedimento é feito com o comando `cvs update`. Em seguida, os dados devem ser enviados de volta ao repositório com o comando `cvs commit`. Depois de compreender esse procedimento, os usuários principiantes também serão capazes de usar o CVS com facilidade.

26.2.10 Segurança contra ataques

Durante a transmissão, o ideal é proteger os dados contra interceptação e manipulação. É muito fácil usar o CVS e o rsync por SSH (shell seguro), proporcionando segurança contra ataques desse tipo. A execução do CVS via rsh (remote shell) deve ser evitada. O acesso ao CVS com o mecanismo *pserver* em redes desprotegidas também não é recomendável.

26.2.11 Proteção contra perda de dados

O CVS tem sido usado por desenvolvedores por um longo tempo para gerenciar projetos de programas e é extremamente estável. Como o histórico do desenvolvimento é gravado, o CVS fornece proteção até mesmo contra certos erros do usuário, como uma exclusão não intencional de um arquivo.

TABELA 26.1 RECURSOS DAS FERRAMENTAS DE SINCRONIZAÇÃO DE ARQUIVOS: -- = MUITO RUIM, - = RUIM OU INDISPONÍVEL, O = MÉDIO, + = BOM, ++ = EXCELENTE, X = DISPONÍVEL

	CVS	**rsync**
Cliente/Servidor	C-S	C-S
Portabilidade	Lin,Un*x,Win	Lin,Un*x,Win
Interatividade	x	x
Velocidade	o	+
Conflitos	+ +	o
Sel. de arquivos	Sel./arq., dir.	Dir.
Histórico	x	-
Espaço em disco rígido	--	o
Interface gráfica do usuário (GUI)	o	-
Dificuldade	o	+
Ataques	+ (SSH)	+ (SSH)

	CVS	rsync
Perda de dados	+ +	+

26.3 Introdução ao CVS

O CVS é adequado para fins de sincronização, caso arquivos específicos sejam editados com frequência e sejam armazenados em um formato de arquivo, como texto ASCII, ou como texto de origem de programa. O uso do CVS para sincronizar dados em outros formatos (como arquivos JPEG) é possível, mas gera grandes volumes de dados, pois todas as variantes de um arquivo ficam armazenadas permanentemente no servidor CVS. Nesses casos, não é possível usar a maioria dos recursos do CVS. O uso do CVS para sincronizar arquivos só será possível se todas as estações de trabalho puderem acessar o mesmo servidor.

26.3.1 Configurando um servidor CVS

O *servidor* é o host em que todos os arquivos válidos se localizam, incluindo as versões mais recentes de todos os arquivos. Qualquer estação de trabalho estacionária pode ser usada como um servidor. Se possível, os dados do repositório do CVS devem ser incluídos em backups regulares.

Durante a configuração de um servidor CVS, é uma boa ideia conceder aos usuários o acesso ao servidor via SSH. Se o usuário for conhecido pelo servidor como `tux` e o software do CVS estiver instalado tanto no servidor quanto no cliente, as variáveis de ambiente a seguir deverão ser definidas no lado do cliente:

```
CVS_RSH=ssh CVSROOT=tux@server:/serverdir
```

O comando **`cvs`** `init` pode ser usado para inicializar o servidor CVS no lado cliente. Esse procedimento deve ser executado apenas uma vez.

Finalmente, é necessário designar um nome à sincronização. Selecione ou crie um diretório no cliente para conter arquivos a serem gerenciados com o CVS (o diretório também pode ficar vazio). O nome do diretório também será o nome da sincronização. Neste exemplo, o diretório é chamado de `synchome`. Vá para esse diretório e digite o comando a seguir para definir o nome de sincronização como `synchome`:

```
cvs import synchome tux wilber
```

Vários comandos do CVS requerem um comentário. Para essa finalidade, o CVS inicia um editor (o editor definido na variável do ambiente `$EDITOR` ou vi, se nenhum editor tiver sido definido). A chamada do editor pode ser evitada se você inserir o comentário antes na linha de comando, como no exemplo a seguir:

```
cvs import -m 'this is a test' synchome tux wilber
```

26.3.2 Usando o CVS

O repositório de sincronização agora pode ter a saída registrada de todos os hosts com **`cvs`** `co synchome`. Esse procedimento cria um novo subdiretório `synchome` no cliente. Para confirmar suas mudanças ao servidor, vá para o diretório `synchome` (ou um de seus subdiretórios) e digite **`cvs`** `commit`.

Por padrão, todos os arquivos (incluindo subdiretórios) são confirmados no servidor. Para confirmar apenas determinados arquivos ou diretórios individuais, especifique-os como em **`cvs`** `commit arquivo1 diretório1`. É necessário adicionar novos arquivos e diretórios ao repositório com um comando como **`cvs`** `add arquivo1 diretório1` antes de confirmá-los no servidor. Depois disso, confirme os arquivos e diretórios recém-adicionados com **`cvs`** `commit arquivo1 diretório1`.

Se você for para outra estação de trabalho, registre a saída do repositório de sincronização, caso isso não tenha sido feito em uma sessão anterior na mesma estação de trabalho.

Inicie a sincronização com o servidor com **`cvs`** `update`. Atualize arquivos ou diretórios individuais como em **`cvs`** `update arquivo1 diretório1`. Para ver a diferença entre os arquivos atuais e versões armazenadas no servidor, use o comando **`cvs`** `diff` ou **`cvs`** `diff arquivo1 diretório1`. Use **`cvs`** `-nq update` para ver quais arquivos podem ser afetados por uma atualização.

Estes são alguns símbolos de status exibidos durante uma atualização:

U

A versão local foi atualizada. Isso afeta todos os arquivos fornecidos pelo servidor e ausentes no sistema local.

M

A versão local foi modificada. Se havia mudanças no servidor, foi possível fundir as diferenças na cópia local.

P

A versão local foi corrigida com a versão do servidor.

C

O arquivo local está em conflito com a versão atual do repositório.

?

Este arquivo não existe no CVS.

O status `M` indica um arquivo modificado localmente. Envie a cópia local para o servidor ou remova o arquivo local e execute a atualização novamente. Nesse caso, o arquivo ausente será recuperado do servidor. Se você enviar um arquivo modificado localmente e ele tiver sido mudado na mesma linha de comando e enviado, poderá haver um conflito, indicado por `C`.

Nesse caso, observe as marcas de conflito ("`>>`" e "`<<`") no arquivo e decida-se entre as duas versões. Como essa tarefa pode ser desagradável, você pode abandonar as mudanças, apagar o arquivo local e digitar **`cvs`** `up` para recuperar a versão atual do servidor.

26.4 Introdução ao rsync

O rsync será útil quando for necessário transmitir grandes quantidades de dados regularmente, sem que haja muitas mudanças. Esse é, por exemplo, sempre o caso da criação de backups. Uma outra aplicação diz respeito a servidores para teste. Esses servidores armazenam árvores completas de diretório de servidores Web regularmente espelhadas em um servidor Web em um DMZ.

26.4.1 Configuração e operação

O rsync pode ser operado em dois modos diferentes. Ele pode ser usado para arquivar ou copiar dados. Para fazer isso, apenas um shell remoto, como o SSH, é necessário no sistema de destino. Entretanto, o rsync também pode ser usado como um daemon para fornecer diretórios à rede.

O modo de operação básica do rsync não requer qualquer configuração especial. O rsync permite diretamente o espelhamento de diretórios inteiros em outro sistema. Como exemplo, o comando a seguir cria um backup do diretório pessoal do tux em um servidor de backup chamado de sun:

```
rsync -baz -e ssh /home/tux/ tux@sun:backup
```

O comando a seguir é usado para reproduzir o diretório de volta:

```
rsync -az -e ssh tux@sun:backup /home/tux/
```

Até esse ponto, o gerenciamento não é muito diferente do de uma ferramenta de cópia comum, como o scp.

O rsync deve ser operado no modo “rsync” para que todos os recursos fiquem totalmente disponíveis. Isso é feito ao se iniciar o daemon rsyncd em mais de um sistema. Configure-o no arquivo `/etc/rsyncd.conf`. Por exemplo, para tornar o diretório `/srv/ftp` disponível com o rsync, use a seguinte configuração:

```
gid = nobody
uid = nobody
read only = true
use chroot = no
transfer logging = true
log format = %h %o %f %l %b
log file = /var/log/rsyncd.log

[FTP]
        path = /srv/ftp
        comment = An Example
```

Em seguida, reinicie o rsyncd com **`systemctl start rsyncd.service`**. É possível também iniciar o rsyncd automaticamente durante o processo de boot. Para essa configuração, ative esse serviço no *Gerenciador de Serviços* do YaST ou manualmente, digitando o comando:

```
root #  systemctl enable rsyncd.service
```

Se preferir, inicie o syncd pelo xinetd. Entretanto, isso só é recomendável para servidores que raramente usam o rsyncd.

O exemplo também cria um arquivo de registro listando todas as conexões. Esse arquivo é armazenado em `/var/log/rsyncd.log`.

Então será possível testar a transferência de um sistema cliente. Faça isso com o seguinte comando:

```
rsync -avz sun::FTP
```

Esse comando lista todos os arquivos presentes no diretório `/srv/ftp` do servidor. Essa solicitação também é registrada no arquivo de registro `/var/log/rsyncd.log`. Para iniciar uma transferência real, forneça um diretório de destino. Use `.` para o diretório atual. Por exemplo:

```
rsync -avz sun::FTP .
```

Por padrão, nenhum arquivo será apagado durante a sincronização com o rsync. Se esse procedimento for forçado, a opção adicional `--delete` deverá ser expressa. Para garantir que nenhum arquivo novo seja apagado, use a opção `--update` como alternativa. Qualquer conflito ocorrido deve ser resolvido manualmente.

26.5 Para obter mais informações

CVS

Você encontra informações importantes sobre o CVS na home page http://www.cvshome.org.

rsync

Informações importantes sobre o rsync são fornecidas nas páginas de manual `man rsync` e `man rsyncd.conf`. Uma referência técnica sobre os princípios de operação do rsync pode ser encontrada em `/usr/share/doc/packages/rsync/tech_report.ps`. As notícias mais recentes sobre o rsync encontram-se no site do projeto na Web, em http://rsync.samba.org/.

Subversion

O Subversion está disponível no SDK do SUSE Linux Enterprise. O SDK é um produto complementar do SUSE Linux Enterprise e está disponível para download pelo site http://download.suse.com/. Pesquise por `SUSE Linux Enterprise Software Development Kit`.

IV Computadores móveis

27 Computação móvel com o Linux 367

28 Gerenciamento de energia 379

27 Computação móvel com o Linux

A computação móvel é geralmente associada a laptops, PDAs e telefones celulares (e ao intercâmbio de dados entre esses aparelhos). Os componentes de hardware móvel, como discos rígidos externos, discos flash ou câmeras digitais, podem ser conectados a laptops ou sistemas desktop. Vários componentes de software estão envolvidos em cenários de computação e alguns aplicativos são desenvolvidos para uso móvel.

27.1 Laptops

O hardware de laptops difere do hardware de um sistema de desktop normal. Isso se deve a critérios como permutabilidade, requisitos de espaço e consumo de energia, que devem ser levados em conta. Os fabricantes de hardware móvel desenvolveram interfaces padrão, como PCMCIA (Personal Computer Memory Card International Association), Mini PCI e Mini PCIe, que podem ser usadas para estender o hardware de laptops. Os padrões englobam cartões de memória, placas de interface de rede e discos rígidos externos.

27.1.1 Conservação de energia

A inclusão de componentes de sistema com otimização de energia durante a fabricação de laptops contribui para a sua adequação ao uso sem acesso à rede elétrica. A contribuição desses componentes para a preservação de energia é, ao menos, tão importante quanto a do sistema operacional. O SUSE® Linux Enterprise Desktop suporta vários métodos que influenciam o consumo de energia de um laptop e possuem diversos efeitos sobre o tempo de operação durante o uso de energia da bateria. A lista a seguir está em ordem decrescente de contribuição para a conservação de energia:

- Regulagem da velocidade da CPU.
- Desativação da iluminação da tela durante pausas.
- Ajuste manual da iluminação da tela.
- Desconexão de acessórios não utilizados, habilitados para HotPlug (CD-ROM USB, mouse externo, placas PCMCIA não usadas, Wi-Fi, etc.).
- Colocação do disco rígido em modo de espera quando inativo.

Você encontra informações detalhadas sobre o gerenciamento de energia do SUSE Linux Enterprise Desktop no *Capítulo 28, Gerenciamento de energia*.

27.1.2 Integração em ambientes operacionais variáveis

Seu sistema precisa se adaptar a ambientes operacionais variáveis quando for usado para a computação móvel. Vários serviços dependem do ambiente, e os clientes subjacentes precisam ser reconfigurados. O SUSE Linux Enterprise Desktop administra esta tarefa para você.

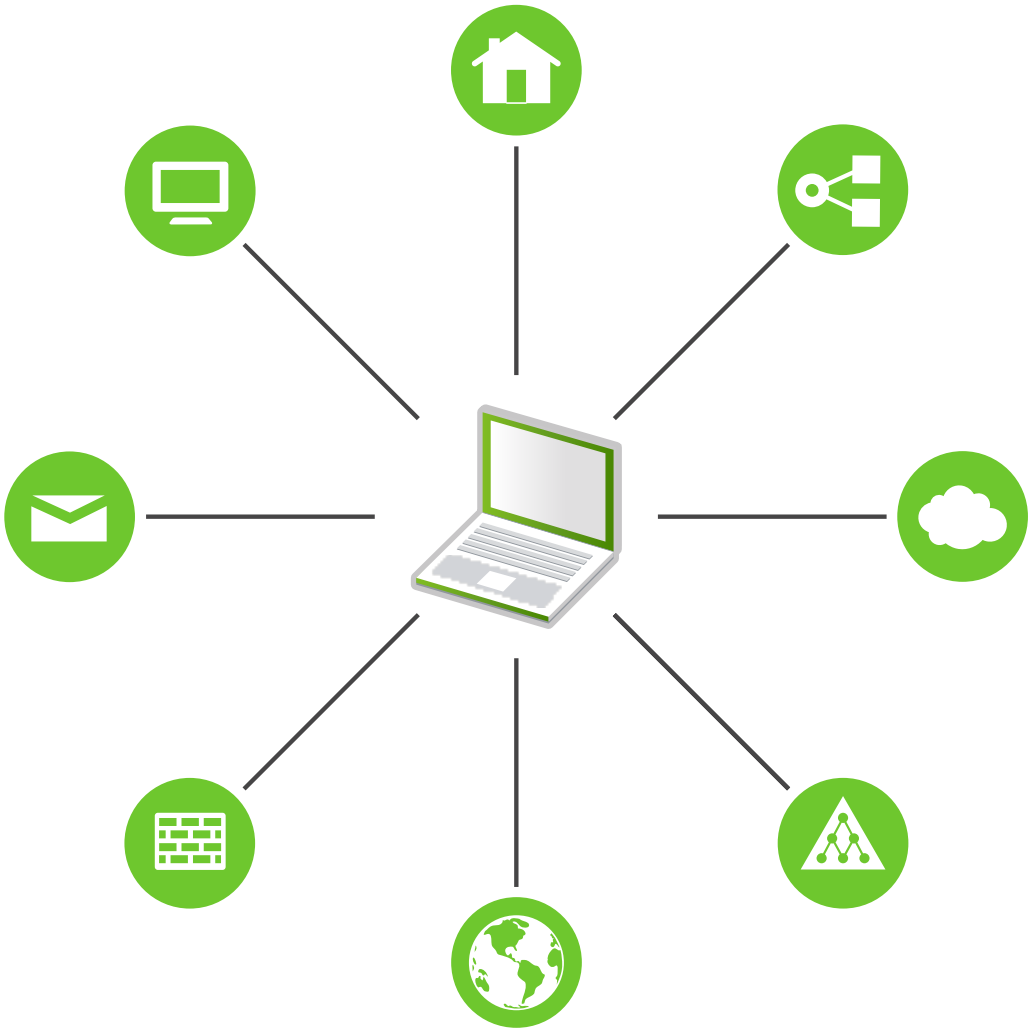


FIGURA 27.1 INTEGRANDO UM COMPUTADOR MÓVEL EM UM AMBIENTE EXISTENTE

Os serviços afetados no caso de um laptop que transita entre uma pequena rede doméstica e uma rede de escritório são:

Rede

Inclui a atribuição de endereço IP, a resolução do nome, a conectividade à Internet e a conectividade a outras redes.

Impressão

Precisam estar presentes um banco de dados atual de impressoras disponíveis e um servidor de impressão disponível, dependendo da rede.

E-mail e proxies

Assim como ocorre com a impressão, a lista dos servidores correspondentes precisa ser atual.

X (ambiente gráfico)

Se o seu laptop estiver temporariamente conectado a um projetor ou monitor externo, configurações de exibição diferentes precisam estar disponíveis.

O SUSE Linux Enterprise Desktop oferece várias maneiras de integrar laptops a ambientes operacionais existentes:

NetworkManager

O NetworkManager é desenvolvido especialmente para rede móvel em laptops. Oferece meios para troca fácil e automática de ambientes de rede ou tipos de rede diferentes como banda larga móvel (por exemplo, GPRS, EDGE ou 3G), LAN wireless e Ethernet. O NetworkManager suporta criptografia WEP e WPA-PSK em LANs wireless. Ele também suporta conexões discadas. A área de trabalho do GNOME inclui um front end para o NetworkManager. Para obter mais informações, consulte a *Seção 22.3, “Configurando conexões de rede”*.

TABELA 27.1 CASOS DE USO PARA O NETWORKMANAGER

Meu computador…	Usar NetworkManager
é um laptop	Sim
algumas vezes está conectado a redes diferentes	Sim

Meu computador...	Usar NetworkManager
fornece serviços de rede (como DNS ou DHCP)	Não
usa somente um endereço IP estático	Não

Use as ferramentas do YaST para configurar a rede sempre que o NetworkManager não deve gerenciar a configuração de rede.

Dica: configuração DNS e vários tipos de conexões de rede

Se você viaja bastante com seu laptop e sempre muda para tipos de conexões de rede diferentes, o NetworkManager funcionará muito bem quando todos os endereços DNS forem atribuídos corretamente com DHCP. Se algumas das suas conexões usarem endereço(s) DNS estático(s), adicione-as à opção `NETCONFIG_DNS_STATIC_SERVERS` em `/etc/sysconfig/network/config`.

SLP

O SLP (Service Location Protocol) simplifica a conexão de um laptop a uma rede existente. Sem o SLP, o administrador do laptop normalmente necessita ter conhecimentos detalhados sobre os serviços disponíveis em uma rede. O SLP transmite a disponibilidade de um determinado tipo de serviço a todos os clientes de uma rede local. Os aplicativos que dão suporte ao SLP podem processar as informações despachadas pelo SLP e podem ser configurados automaticamente. O SLP também pode ser usado para instalar um sistema, minimizando o esforço de procurar uma fonte de instalação adequada.

27.1.3 Opções de software

Várias áreas de tarefas especiais no uso móvel ficam a cargo de software dedicado: monitoração do sistema (especialmente a carga da bateria), sincronização de dados e comunicação wireless com periféricos e com a Internet. As seguintes seções apresentam os aplicativos mais importantes que o SUSE Linux Enterprise Desktop oferece para cada tarefa.

27.1.3.1 Monitoração do sistema

Há duas ferramentas de monitoramento de sistema incluídas no SUSE Linux Enterprise Desktop:

Gerenciamento de Energia

Gerenciamento de Energia é um aplicativo que permite ajustar o comportamento relacionado à economia de energia da área de trabalho do GNOME. Normalmente, você pode acessá-lo em *Computador* › *Centro de Controle* › *Sistema* › *Gerenciamento de Energia*.

Monitor do Sistema

O *Monitor do Sistema* reúne os parâmetros mensuráveis do sistema em um ambiente de monitoramento. Por padrão, ele apresenta as informações de saída em três guias. *Processos* mostra informações detalhadas sobre os processos que estão em execução, como carga da CPU, uso da memória ou número do ID e prioridade do processo. É possível personalizar a apresentação e filtragem dos dados coletados: para adicionar informações sobre um novo tipo de processo, clique no cabeçalho da tabela do processo e escolha qual coluna ocultar ou adicionar à tela. É possível também monitorar diferentes parâmetros do sistema em diversas páginas de dados ou coletar os dados de diversas máquinas em paralelo na rede. A guia *Recursos* mostra os gráficos da CPU, a memória e o histórico de rede, e a guia *Sistema de Arquivos* lista todas as partições e seu uso.

27.1.3.2 Sincronizando dados

Ao alternar entre o trabalho em uma máquina móvel desconectada da rede e o trabalho em uma estação em rede em um escritório, é necessário manter a sincronização dos dados processados em todas as instâncias. Isso pode incluir pastas de e-mail, diretórios e arquivos individuais que precisam estar presentes tanto para o trabalho remoto como para o trabalho no escritório. A solução nos dois casos é a seguinte:

Sincronizando e-mail

Use uma conta IMAP para armazenar seus e-mails na rede empresarial. Em seguida, acesse os e-mails da estação de trabalho usando qualquer cliente de e-mail habilitado para IMAP desconectado, como o Mozilla Thunderbird Mail ou o Evolution , conforme descrito no *Book* “Guia do Usuário do GNOME” . O cliente de e-mail precisa ser configurado de tal modo que as `Mensagens enviadas` sejam sempre acessadas da mesma pasta. Isso assegura a disponibilidade de todas as mensagens com informações sobre seu status após a conclusão

do processo de sincronização. Use um servidor SMTP implementado no cliente de e-mail para enviar mensagens, em vez do sendmail ou postfix do MTA de todo o sistema para receber um feedback confiável sobre e-mails não enviados.

Sincronizando arquivos e diretórios

Existem diversos utilitários adequados para a sincronização de dados entre um laptop e uma estação de trabalho. Um dos mais usados é uma ferramenta de área de trabalho chamada `rsync`. Para obter mais informações, consulte a respectiva página de manual (`man 1 rsync`).

27.1.3.3 Comunicação wireless: Wi-Fi

Com a enorme variedade de tecnologias wireless, Wi-Fi é a única adequada para a operação de redes grandes e, às vezes, até mesmo separadas geograficamente. Máquinas individuais podem se conectar entre si para formar uma rede wireless independente ou para acessar a Internet. Os dispositivos denominados *pontos de acesso* funcionam como estações de base para os dispositivos habilitados para Wi-Fi e atuam como intermediários no acesso à Internet. Um usuário móvel pode alternar entre pontos de acesso dependendo do local e de que ponto de acesso ofereça a melhor conexão. Como na telefonia celular, uma rede grande está disponível aos usuários de Wi-Fi sem os vincular a um local específico para acessá-la.

As placas Wi-Fi comunicam-se usando o padrão 802.11, preparado pela organização IEEE. Originalmente, esse padrão fornecia uma taxa de transmissão máxima de 2 MBit/s. Enquanto isso, vários suplementos foram adicionados para aumentar a taxa de dados. Esses suplementos definem detalhes como modulação, saída de transmissão e taxas de transmissão (consulte a *Tabela 27.2, "Visão geral dos vários padrões de Wi-Fi"*). Além disso, muitas empresas implementam hardware com recursos proprietários ou preliminares.

TABELA 27.2 VISÃO GERAL DOS VÁRIOS PADRÕES DE WI-FI

Nome (802.11)	Frequência (GHz)	Taxa de transmissão máxima (MBit/s)	Nota
a	5	54	Menos sujeito a interferência
b	2.4	11	Menos comum

Nome (802.11)	Frequência (GHz)	Taxa de transmissão máxima (MBit/s)	Nota
g	2.4	54	Disseminado, compatível retroativamente com 11b
e	2.4 e/ou 5	300	Comum
ac	5	até ~865	Expectativa de se tornar comum em 2015
ad	60	até aprox. 7000	Lançado em 2012, atualmente menos comum; não suportado no SUSE Linux Enterprise Server

As placas 802.11 legadas não são suportadas pelo SUSE® Linux Enterprise Desktop. A maioria das placas que usam 802.11 a/b/g/n é suportada. As placas novas geralmente são compatíveis com o padrão 802.11n, mas as placas que usam 802.11g ainda estão disponíveis.

27.1.3.3.1 Modos de funcionamento

Nas redes sem fio, várias técnicas e configurações são usadas para assegurar conexões rápidas, seguras e com alta qualidade. Na maioria dos casos, a placa Wi-Fi opera no *modo gerenciado*. Entretanto, tipos de operação diferentes precisam de configurações diferentes. É possível classificar as redes wireless em quatro modos de rede:

Modo Gerenciado (Modo Infraestrutura), por Ponto de Acesso (modo padrão)

As redes gerenciadas têm um elemento de gerenciamento: o ponto de acesso. Neste modo (também chamado de modo infraestrutura ou padrão), todas as conexões das estações de Wi-Fi na rede são efetuadas por meio do ponto de acesso, que também pode funcionar

como conexão com uma Ethernet. Para verificar se apenas as estações autorizadas poderão se conectar, vários mecanismos de autenticação (WPA, etc) são usados. Ele é também o principal modo que consome a menor quantidade de energia.

Modo Ad-hoc (Rede Ponto a Ponto)

Redes ad-hoc não possuem um ponto de acesso. As estações se comunicam diretamente umas com as outras, portanto, uma rede ad hoc geralmente é mais lenta do que uma rede gerenciada. Entretanto, a faixa de transmissão e o número de estações participantes são muito limitados nas redes ad-hoc. Elas também não suportam autenticação WPA. Se você pretende usar segurança WPA, não convém usar o modo ad hoc. Saiba que nem todas as placas suportam o modo ad hoc de maneira confiável.

Modo Master

No modo master, a placa Wi-Fi é usada como o ponto de acesso, supondo que a placa suporte esse modo. Confira os detalhes de sua placa Wi-Fi em http://linux-wless.passys.nl.

Modo de Malha

As redes de malha wireless são organizadas em uma *topologia em malha*. A conexão de uma rede de malha wireless é distribuída entre todos os *nós* de malha wireless. Cada nó pertencente à rede é conectado a outros nós para compartilhar a conexão, possivelmente englobando uma grande área.

27.1.3.3.2 Autenticação

Como uma rede sem fio é muito mais fácil de interceptar e comprometer do que uma rede com fio, os vários padrões incluem métodos de autenticação e criptografia.

As placas Wi-Fi antigas suportam apenas WEP (Wired Equivalent Privacy – Privacidade Equivalente à de Redes com Fio). No entanto, como o WEP não se provou seguro, a indústria de Wi-Fi definiu uma extensão chamada WPA, que supostamente elimina as vulnerabilidades do WEP. O WPA, às vezes sinônimo de WPA2, deve ser o método de autenticação padrão.

Em geral, o usuário não pode escolher nenhum método de autenticação, na maioria dos casos. Por exemplo, quando uma placa opera no modo gerenciado, a autenticação é definida pelo ponto de acesso. O NetworkManager mostra o método de autenticação.

27.1.3.3.3 Criptografia

Existem vários métodos de criptografia para assegurar que pessoas não autorizadas não possam ler os pacotes de dados que são trocados em uma rede sem fio nem obter acesso à rede:

WEP (definido no padrão IEEE 802.11)

Esse padrão utiliza o algoritmo de criptografia RC4, originalmente com um tamanho de chave de 40 bits, posteriormente também com 104 bits. Muitas vezes, o tamanho é declarado como 64 bits ou 128 bits, dependendo da inclusão ou não dos 24 bits do vetor de inicialização. Porém, esse padrão tem algumas fraquezas. Os ataques contra as chaves geradas por esse sistema podem ser bem-sucedidos. Contudo, é melhor usar o WEP do que não criptografar a rede de maneira alguma.

Alguns fornecedores implementaram o "WEP Dinâmico" não padrão. Ele funciona exatamente como o WEP e compartilha os mesmos pontos fracos, exceto pelo fato de que a chave é mudada periodicamente por um serviço de gerenciamento de chave.

TKIP (definido no padrão WPA/IEEE 802.11i)

Esse protocolo de gerenciamento de chave definido no padrão WPA utiliza o mesmo algoritmo de criptografia do WEP, mas elimina sua fraqueza. Como uma nova chave é gerada para cada pacote de dados, os ataques contra essas chaves são infrutíferos. O TKIP é usado junto com o WPA-PSK.

CCMP (definido no padrão IEEE 802.11i)

O CCMP descreve o gerenciamento de chave. Normalmente, ele é usado na conexão com o WPA-EAP, mas também pode ser usado com o WPA-PSK. A criptografia acontece de acordo com o AES e é mais forte do que a criptografia RC4 do padrão WEP.

27.1.3.4 Comunicação wireless: Bluetooth

Entre todas as tecnologias wireless, o Bluetooth é a que possui o mais amplo espectro de aplicação. Ele pode ser usado na comunicação entre computadores (laptops) e PDAs ou telefones celulares, assim como o IrDA. Também pode ser utilizado para conectar diversos computadores dentro de uma extensão. O bluetooth também é usado para conectar componentes wireless do sistema, como um teclado ou mouse. Entretanto, o alcance dessa tecnologia não é suficiente para conectar sistemas remotos a uma rede. Wi-Fi é a tecnologia preferida para comunicação através de obstáculos físicos, como paredes.

27.1.3.5 Comunicação wireless: IrDA

O IrDA é a tecnologia wireless de menor alcance. As duas extremidades da comunicação precisam estar a uma distância visível uma da outra. Não é possível contornar obstáculos como paredes. Uma aplicação possível do IrDA é a transmissão de arquivos de um laptop para um telefone celular. O curto caminho do laptop para o telefone celular é coberto com o uso do IrDA. A transmissão de longo alcance do arquivo para o destinatário é efetuada pela rede móvel. Outra aplicação do IrDA é a transmissão wireless de serviços de impressão no escritório.

27.1.4 Segurança de dados

Em termos ideais, os dados contidos no seu laptop são protegidos de diversas maneiras contra o acesso não autorizado. Possíveis medidas de segurança podem ser tomadas nas seguintes áreas:

Proteção contra roubo

Sempre que possível proteja a integridade física do seu sistema contra roubo. Diversas ferramentas de segurança (como correntes) podem ser adquiridas em lojas varejistas.

Autenticação avançada

Use a autenticação biométrica juntamente com a autenticação padrão por meio de login e senha. O SUSE Linux Enterprise Desktop suporta autenticação por impressão digital.

Protegendo dados no sistema

Dados importantes devem ser criptografados não apenas durante a transmissão, mas também no disco rígido. Essa medida assegura sua segurança em caso de roubo. A criação de uma partição criptografada com o SUSE Linux Enterprise Desktop está descrita no *Book "Security Guide" 11 "Encrypting Partitions and Files"*. Outra possibilidade é criar diretórios pessoais criptografados ao adicionar o usuário com o YaST.

Importante: segurança de dados e o evento Suspender para Disco

As partições criptografadas não são desmontadas durante um evento de suspender para disco. Assim, todos os dados contidos nessas partições ficarão disponíveis para qualquer pessoa que conseguir roubar o hardware e inicializar o disco rígido.

Segurança da rede

Qualquer transferência de dados deve ser segura, não importando como a transferência é feita. Para obter mais informações sobre problemas gerais de segurança referentes ao Linux e redes, consulte o *Book "*Security Guide*" 1 "Security and Confidentiality"*.

27.2 Hardware móvel

O SUSE Linux Enterprise Desktop suporta detecção automática de dispositivos de armazenamento móveis por FireWire (IEEE 1394) ou USB. O termo *dispositivo de armazenamento móvel* se aplica a qualquer tipo de disco rígido FireWire ou USB, unidade flash USB ou câmera digital. Esses dispositivos são automaticamente detectados e configurados logo após serem conectados ao sistema pela interface correspondente. O gerenciador de arquivos do GNOME oferece manipulação flexível de itens de hardware móvel. Para desmontar esse tipo de mídia com segurança, use o recurso *Desmontar Volume* (GNOME) do gerenciador de arquivos. Para obter mais detalhes, consulte o *Book "*Guia do Usuário do GNOME*"* .

Discos rígidos externos (USB e FireWire)

Assim que o disco rígido externo for corretamente reconhecido pelo sistema, seu ícone aparecerá no gerenciador de arquivos. Clique no ícone para exibir o conteúdo da unidade. É possível criar diretórios e arquivos aqui e editá-los ou apagá-los. Para mudar o nome original de um disco rígido dado pelo sistema, selecione o item de menu correspondente no menu que aparece ao clicar o botão direito do mouse no ícone. Essa mudança de nome é limitada à exibição no gerenciador de arquivos. O descritor através do qual o dispositivo é montado em `/media` permanece não afetado por isso.

Discos Flash USB

Estes dispositivos são manipulados pelo sistema como discos rígidos externos. Também nesses dispositivos é possível renomear as entradas do gerenciador de arquivos.

Câmeras digitais (USB e FireWire)

As câmeras digitais reconhecidas pelo sistema também aparecem como unidades externas na visão geral do gerenciador de arquivos. É possível processar as imagens usando o F-Spot. Para o processamento avançado de fotos, use o GIMP. Para ver uma breve introdução sobre o GIMP, consulte o *Book "*Guia do Usuário do GNOME*" 18 "GIMP: manipulando gráficos"*.

27.3 Telefones celulares e PDAs

Tanto um sistema de desktop como um laptop podem se comunicar com um telefone celular via Bluetooth ou IrDA. Alguns modelos dão suporte aos dois protocolos; outros, somente a um dos dois. As áreas de uso dos dois protocolos e a extensa documentação correspondente já foram citadas na *Seção 27.1.3.3, "Comunicação wireless: Wi-Fi"*. A configuração desses protocolos nos telefones celulares é descrita nos respectivos manuais.

27.4 Para obter mais informações

O ponto central de referência para todas as dúvidas relativas a dispositivos móveis e o Linux é http://tuxmobil.org/. Diversas seções desse site da Web tratam de aspectos de hardware e software de laptops, PDAs, telefones celulares e outros hardwares móveis.

Uma abordagem semelhante de http://tuxmobil.org/ é feita por http://www.linux-on-laptops.com/. Informações sobre laptops e dispositivos portáteis podem ser encontradas nesse local.

O SUSE mantém uma lista de discussão em alemão dedicada a laptops. Consulte http://lists.opensuse.org/opensuse-mobile-de/. Nesta lista, usuários e desenvolvedores discutem todos os aspectos da computação móvel com SUSE Linux Enterprise Desktop. As mensagens em inglês são respondidas, mas a maioria das informações dos arquivos está disponível somente em alemão. Use http://lists.opensuse.org/opensuse-mobile/ para ver postagens em inglês.

28 Gerenciamento de energia

O gerenciamento de energia é especialmente importante em laptops, mas também é útil em outros sistemas. A ACPI (Advanced Configuration and Power Interface — Interface de Energia e Configuração Avançada) está disponível em todos os computadores modernos (laptops, desktops e servidores). As tecnologias de gerenciamento de energia exigem hardware adequado e rotinas BIOS. A maioria dos laptops e muitos desktops e servidores modernos atendem a esses requisitos. Também é possível controlar a escala de frequência de CPU para economizar energia ou reduzir o ruído.

28.1 Funções de economia de energia

As funções de economia de energia não são significativas apenas para o uso móvel de laptops, como também para sistemas desktop. As funções principais e respectivas utilizações na ACPI são:

Standby

Não suportado.

Suspender (para memória)

Este modo grava todo o estado do sistema na memória RAM. Em seguida, todo o sistema é colocado em repouso, salvo a memória RAM. Neste estado, o computador consome pouquíssima energia. A vantagem desse estado é a possibilidade de reiniciar o trabalho no mesmo ponto em alguns segundos sem precisar inicializar e reiniciar os aplicativos. Essa função corresponde ao estado da ACPI `S3`.

Suspender (para o disco)

Neste modo operacional, o estado do sistema inteiro é gravado no disco rígido e o sistema é desligado. Deve existir uma partição de troca pelo menos tão grande quanto a RAM para gravar todos os dados ativos. A reativação desse estado leva de 30 a 90 segundos. O estado anterior ao suspenso é restaurado. Alguns fabricantes oferecem variantes híbridas desse modo, como RediSafe em Thinkpads da IBM. O estado correspondente da ACPI é `S4`. No Linux, a suspensão para disco é desempenhada pelas rotinas de kernel, que são independentes de ACPI.

Monitor de bateria

A ACPI verifica o status da carga da bateria e fornece informações correspondentes. Além disso, ela coordena as ações a serem desempenhadas quando um status de carga crítico é atingido.

Desligamento automático

Após um encerramento, o computador é desligado. Isto é especialmente importante quando um encerramento automático é realizado pouco antes da bateria esgotar-se.

Controle de velocidade do processador

Em conexão com a CPU, é possível economizar energia de três maneiras diferentes: escala de frequência e voltagem (também conhecida como PowerNow! ou Speedstep), throttling e adormecimento do processador (C-states). Dependendo do modo operacional do computador, esses métodos também podem ser combinados.

28.2 Advanced Configuration and Power Interface (ACPI)

A ACPI foi desenvolvida para habilitar o sistema operacional a configurar e controlar cada componente de hardware. A ACPI substitui tanto o Plug and Play (PnP) de Gerenciamento de Energia quanto o Gerenciamento Avançado de Energia (APM). Ela envia informações sobre a bateria, o adaptador de CA, a temperatura, o ventilador e eventos do sistema, como “fechar tampa” ou “bateria fraca”.

O BIOS fornece tabelas que contém informações sobre os componentes individuais e métodos de acesso ao hardware. O sistema operacional usa essas informações para tarefas como atribuir interrupções ou ativar e desativar componentes. Como o sistema operacional executa comandos armazenados no BIOS, a funcionalidade depende da implementação do BIOS. As tabelas que a ACPI pode detectar e carregar estão relatadas em journald. Consulte o *Capítulo 12, `journalctl`: consultar o diário do `systemd`* para obter mais informações sobre como ver as mensagens de registro do diário. Consulte a *Seção 28.2.2, “Solução de problemas”* para obter mais informações sobre solução de problemas da ACPI.

28.2.1 Controlando o desempenho da CPU

A CPU pode economizar energia de três maneiras:

- Escala de frequência e voltagem
- Obstruindo a frequência do relógio (T-states)
- Adormecendo o processador (C-states)

Dependendo do modo operacional do computador, estes métodos também podem ser combinados. Economizar energia também significa que o sistema esquenta menos e os ventiladores são ativados com menos frequência.

Expansão e throttling de frequência são relevantes apenas quando o processador está ocupado, pois o C-state mais econômico é aplicado de qualquer maneira quando o processador fica ocioso. Se a CPU estiver ocupada, a escala da frequência é o método recomendado para economia de energia. Em geral o processador só trabalha com carga parcial. Neste caso, pode ser executado com uma frequência inferior. Normalmente, a expansão da frequência dinâmica controlada pelo regulador sob demanda do kernel é a melhor abordagem.

Throttling deve ser usado como última alternativa, por exemplo, para ampliar o tempo de operação da bateria, apesar de uma alta carga do sistema. Contudo, alguns sistemas não são executados suavemente quando ocorrem throttlings em excesso. Ademais, o throttling da CPU não faz sentido se a CPU tem pouco a fazer.

Para obter informações mais detalhadas, consulte o *Book* “System Analysis and Tuning Guide” *10 “Power Management”*.

28.2.2 Solução de problemas

Há dois tipos de problemas. De um lado, o código ACPI do kernel pode conter erros que não foram detectados em tempo útil. Neste caso, uma solução estará disponível para download. O mais comum é que os problemas sejam causados pelo BIOS. Às vezes, desvios da especificação da ACPI são propositalmente integrados ao BIOS para contornar erros na implementação da ACPI em outros sistemas operacionais amplamente utilizados. Componentes de hardware que têm erros sérios na implementação da ACPI são gravados em uma lista negra que impede que o kernel do Linux use a ACPI para esses componentes.

A primeira ação a ser tomada quando problemas forem detectados, é atualizar o BIOS. Se o computador não inicializar de jeito nenhum, um dos seguintes parâmetros de boot poderá ser útil:

pci=noacpi

Não usar ACPI para configurar os dispositivos PCI.

acpi=ht

Realizar apenas uma configuração com recursos simples. Não usar a ACPI para outros fins.

acpi=off

Desabilitar a ACPI.

Atenção: problemas de boot sem ACPI

Algumas máquinas mais novas (especialmente os sistemas SMP e AMD64) precisam de ACPI para configurar o hardware corretamente. Nestas máquinas, desabilitar a ACPI pode causar problemas.

Às vezes a máquina é confundida pelo hardware conectado por USB ou FireWire. Se uma máquina se recusa a inicializar, desconecte todos os itens de hardware desnecessários e tente novamente.

Monitore as mensagens de boot do sistema com o comando `dmesg -T | grep -2i acpi` (ou todas as mensagens, porque o problema pode não ser causado pela ACPI) após a inicialização. Se ocorrer um erro ao analisar uma tabela ACPI, a tabela mais importante, a DSDT (*Differentiated System Description Table*), poderá ser substituída por uma versão aprimorada. Neste caso, a DSDT defeituosa do BIOS é ignorada. O procedimento está descrito na *Seção 28.4, “Solução de problemas”*.

Na configuração do kernel, há um switch para ativar as mensagens de depuração da ACPI. Se houver um kernel com depuração ACPI compilado e instalado, serão emitidas informações detalhadas.

Se você tiver problemas com BIOS ou hardware, é sempre recomendável entrar em contato com os fabricantes. Especialmente se eles nem sempre derem assistência ao Linux, devem ser indagados em caso de problemas. Os fabricantes só levarão a questão a sério se compreenderem que um número satisfatório de seus clientes usa Linux.

28.2.2.1 Para obter mais informações

- http://tldp.org/HOWTO/ACPI-HOWTO/ (ACPI HOWTO detalhado, contém patches DSDT)
- http://www.acpi.info (Configuração Avançada e Especificação da Interface de Energia)
- http://acpi.sourceforge.net/dsdt/index.php (Patches DSDT por Bruno Ducrot)

28.3 Descanso do disco rígido

No Linux, o disco rígido pode colocado em repouso total se não estiver em uso e pode ser executado em modo mais econômico ou silencioso. Nos laptops modernos, não é necessário desativar o disco rígido manualmente, porque entram automaticamente em um modo operacional econômico sempre que não estão em uso. No entanto, para aumentar a economia de energia, experimente alguns dos seguintes métodos usando o comando **`hdparm`**.

Ele pode ser usado para modificar várias configurações de disco rígido. A opção `-y` alterna instantaneamente o disco rígido para o modo standby. `-Y` coloca-o em repouso. **`hdparm`** `-S x` faz o disco rígido ser encerrado após um determinado período de inatividade. Substitua *`x`* conforme a seguir: `0` desabilita esse mecanismo, fazendo o disco rígido funcionar continuamente. Valores de `1` a `240` são multiplicados por 5 segundos. Valores de `241` a `251` correspondem de 1 a 11 vezes 30 minutos.

As opções de economia de energia interna do disco rígido podem ser controladas pela opção `-B`. Selecione um valor de `0` a `255` para obter de economia máxima a throughput máximo. O resultado depende do disco rígido usado e é difícil de avaliar. Para tornar um disco rígido mais silencioso, use a opção `-M`. Selecione um valor de `128` a `254` para obter de silencioso a rápido.

Muitas vezes não é fácil colocar o disco rígido em repouso. No Linux, vários processos gravam no disco rígido, ativando-o repetidamente. Portanto, é importante entender como o Linux trata os dados que necessitam ser gravados no disco rígido. Primeiro, todos os dados estão no buffer da memória RAM. Esse buffer é monitorado pelo daemon `pdflush`. Quando os dados atingem uma determinada idade limite ou quando o buffer está cheio até certo grau, o conteúdo do buffer é descarregado para o disco rígido. O tamanho do buffer é dinâmico e depende do tamanho da

memória e da carga do sistema. Por padrão, pdflush é configurado em intervalos curtos para obter a integridade máxima de dados. Ele verifica o buffer a cada 5 segundos e grava os dados no disco rígido. As seguintes variáveis são interessantes:

`/proc/sys/vm/dirty_writeback_centisecs`
: Inclui o atraso até o thread pdflush ser acionado (em centésimos de segundo).

`/proc/sys/vm/dirty_expire_centisecs`
: Define o período após o qual uma página modificada deve ser gravada por último. O padrão é `3000`, o que equivale a 30 segundos.

`/proc/sys/vm/dirty_background_ratio`
: Porcentagem máxima de páginas modificadas para pdflush começar a gravá-las. O padrão é `5` %.

`/proc/sys/vm/dirty_ratio`
: Quando a página modificada exceder essa porcentagem da memória total, os processos são forçados a gravar buffers modificados durante suas frações de tempo em vez de continuar gravando.

Atenção: deficiência da integridade de dados

Qualquer modificação nas configurações do daemon `pdflush` coloca em risco a integridade dos dados.

Além desses processos, sistemas JFS, como `Btrfs`, `Ext3`, `Ext4` entre outros, gravam seus metadados independentemente do `pdflush`, que também impede que o disco rígido pare de funcionar. Para evitar isso, foi desenvolvida uma extensão especial de kernel para dispositivos móveis. Para usar a extensão, instale o pacote `laptop-mode-tools` e consulte `/usr/src/linux/Documentation/laptops/laptop-mode.txt` para ver os detalhes.

Outro fator importante é o modo como se comportam os programas ativos. Por exemplo, os bons editores gravam regularmente backups ocultos do arquivo modificado no momento para o disco rígido, fazendo com que ele saia do modo de hibernação. Recursos como este podem ser desabilitados às custas da integridade dos dados.

Com relação a isso, o mail daemon postfix faz uso da variável `POSTFIX_LAPTOP`. Se essa variável for configurada para `sim`, postfix acessa o disco rígido com muito menos frequência.

No SUSE Linux Enterprise Desktop, estas tecnologias são controladas por `laptop-mode-tools`.

28.4 Solução de problemas

Todas as mensagens de erro e alertas são registradas no diário do sistema, que pode ser consultado com o comando **`journalctl`** (leia o *Capítulo 12, **`journalctl`**: consultar o diário do `systemd`* para obter mais informações). As seções a seguir abordam os problemas mais comuns.

28.4.1 A frequência da CPU não funciona

Consulte as fontes do kernel para ver se o seu processador é suportado. Você poderá precisar de um módulo de kernel ou de opção especial para ativar o controle de frequência da CPU. Se o pacote `kernel-source` estiver instalado, essas informações estarão disponíveis em `/usr/src/linux/Documentation/cpu-freq/*`.

28.5 Para obter mais informações

- http://en.opensuse.org/SDB:Suspend_to_RAM: Como fazer o recurso Suspender para RAM funcionar
- http://old-en.opensuse.org/Pm-utils: Como modificar a metodologia geral de suspensão

V Solução de problemas

29 Ajuda e documentação 387

30 Problemas comuns e suas soluções 393

29 Ajuda e documentação

O SUSE® Linux Enterprise Desktop vem com várias fontes de informações e documentação, muitas das quais já integradas ao sistema instalado.

Documentação em `/usr/share/doc`

Esse diretório de ajuda tradicional contém vários arquivos de documentação e notas de versão do seu sistema. Também contém informações de pacotes instalados no subdiretório `packages`. Mais informações podem ser encontradas na *Seção 29.1, "Diretório da documentação"*.

Páginas de manual e páginas de informações para comandos do shell

Ao trabalhar com o shell, você não precisa saber de cor as opções de comandos. Tradicionalmente, o shell oferece ajuda integrada por meio das páginas de manual e de informações. Leia mais na *Seção 29.2, "Páginas de manual"* e na *Seção 29.3, "Páginas de informações"*.

Centro de Ajuda da Área de Trabalho

O centro de ajuda da área de trabalho do GNOME (Ajuda) oferece acesso centralizado aos recursos de documentação mais importantes no sistema de forma pesquisável. Esses recursos incluem ajuda online para os aplicativos instalados, páginas de manual, páginas de informações e os manuais do SUSE fornecidos com o produto.

Pacotes de Ajuda separados para alguns aplicativos

Quando um novo software é instalado com o YaST, a documentação do software é instalada automaticamente (na maioria dos casos) e, normalmente, aparece no centro de ajuda da área de trabalho. Porém, alguns aplicativos, como o GIMP, podem ter diversos pacotes de ajuda online que podem ser instalados separadamente com o YaST e que não se integram aos centros de ajuda.

29.1 Diretório da documentação

O diretório tradicional para encontrar a documentação do sistema Linux instalado é `/usr/share/doc`. Geralmente, o diretório contém informações sobre os pacotes instalados no sistema, bem como notas de versão, manuais e muito mais.

Nota: o conteúdo depende dos pacotes instalados

No mundo do Linux, muitos manuais e outros tipos de documentação estão disponíveis na forma de pacotes, como um software. As informações encontradas em `/usr/share/docs` também dependem dos pacotes (de documentação) instalados. Se você não encontrar os subdiretórios mencionados aqui, verifique se os respectivos pacotes estão instalados em seu sistema e adicione-os com o YaST, se necessário.

29.1.1 Manuais do SUSE

Nossos manuais estão disponíveis nas versões em HTML e PDF em vários idiomas. No subdiretório `manual`, você encontra as versões em HTML de quase todos os manuais do SUSE disponíveis para o seu produto. Para obter uma visão geral de toda a documentação disponível para o seu produto, consulte o prefácio dos manuais.

Se houver mais de um idioma instalado, `/usr/share/doc/manual` poderá conter versões em idiomas diferentes dos manuais. As versões em HTML dos manuais do SUSE também estão disponíveis no centro de ajuda de ambas as áreas de trabalho. Para obter informações sobre onde encontrar as versões em PDF e HTML dos manuais na mídia de instalação, consulte as Notas de Versão do SUSE Linux Enterprise Desktop. Elas estão disponíveis no sistema instalado, no diretório `/usr/share/doc/release-notes/`, ou online, na página da Web específica do produto em http://www.suse.com/doc/.

29.1.2 Documentação do pacote

Em `packages`, você encontra a documentação incluída nos pacotes de software instalados no seu sistema. Para qualquer pacote, é criado um subdiretório `/usr/share/doc/packages/`*`nome_do_pacote`*. Ele geralmente contém arquivos README do pacote e às vezes exemplos, arquivos de configuração ou scripts adicionais. A lista a seguir apresenta arquivos típicos encontrados em `/usr/share/doc/packages`. Nenhuma destas entradas é obrigatória, e muitos pacotes podem incluir apenas algumas delas.

`AUTHORS`
: Lista dos principais desenvolvedores.

`BUGS`

Bugs ou falhas conhecidos. Pode conter também um link para uma página do Bugzilla na Web, onde é possível pesquisar todos os bugs.

`CHANGES`, `ChangeLog`

Resumo de mudanças de versão para versão. Geralmente interessante para desenvolvedores, pois é bastante detalhado.

`COPYING`, `LICENSE`

Informações sobre licenciamento.

`FAQ`

Perguntas e respostas coletadas em listas de endereçamento ou grupos de notícias.

`INSTALL`

Como instalar esse pacotes no seu sistema. Visto que o pacote já estará instalado no momento em que você ler este arquivo, você poderá ignorar o conteúdo do arquivo com segurança.

`README`, `README.*`

Informações gerais sobre o software. Por exemplo, a finalidade e o modo de usá-lo.

`TODO`

Itens ainda não implementados, mas que provavelmente serão no futuro.

`MANIFEST`

Lista de arquivos com um breve resumo.

`NEWS`

Descrição do que há de novo nesta versão.

29.2 Páginas de manual

Páginas de manual são uma parte essencial de qualquer sistema Linux. Elas explicam o uso de um comando e todos os parâmetros e opções disponíveis. As páginas de manual podem ser acessadas com **`man`** seguido do nome do comando, por exemplo, **`man ls`**.

As páginas de manual são exibidas diretamente no shell. Para navegar nelas, mova-se para cima e para baixo com Page ↑ e Page ↓. Desloque-se entre o início e o fim do documento com Home e End. Conclua esta exibição pressionando Q. Aprenda mais sobre o próprio comando **man** com **man man**. Páginas de manual são classificadas em categorias, como mostrado na *Tabela 29.1, "Páginas de manual – categorias e descrições"* (extraída da página de manual do próprio comando man).

TABELA 29.1 PÁGINAS DE MANUAL – CATEGORIAS E DESCRIÇÕES

Número	Descrição
1	Programas executáveis ou comandos de shell
2	Chamadas do sistema (funções fornecidas pelo Kernel)
3	Chamadas de biblioteca (funções em bibliotecas de programas)
4	Arquivos especiais (geralmente encontrados em `/dev`)
5	Convenções e formatos de arquivos (`/etc/fstab`)
6	Jogos
7	Diversos (incluindo convenções e pacotes de macro); por exemplo, man(7), groff(7)
8	Comandos de administração de sistema (geralmente, apenas para `root`)
9	Rotinas de kernel (não padrão)

Cada página de manual consiste em várias partes rotuladas *NAME*, *SYNOPSIS*, *DESCRIPTION*, *SEE ALSO*, *LICENSING* e *AUTHOR*. Pode haver seções adicionais disponíveis, dependendo do tipo de comando.

29.3 Páginas de informações

Páginas de informações são outra fonte importante de informações no sistema. Geralmente, elas são mais detalhadas do que as páginas de manual. Elas abrangem mais do que as opções de linha de comando e, às vezes, incluem tutoriais completos ou documentação de referência. Para ver a página de informações de um determinado comando, digite **`info`** seguido pelo nome do comando, por exemplo, **`info ls`**. Você pode procurar uma página de informações com um viewer diretamente no shell e exibir as seções diferentes, denominadas "nós". Use Space para avançar e <- para voltar. Em um nó, você também pode procurar com Page ↑ e Page ↓, mas apenas Space e <- o levarão também para o nó anterior ou subsequente. Pressione Q para sair do modo de visualização. Nem todo comando vem com uma página de informações e vice-versa.

29.4 Recursos Online

Além das versões online dos manuais do SUSE instaladas em `/usr/share/doc`, você também pode acessar a documentação e os manuais específicos do produto na Web. Para uma visão geral de toda a documentação disponível referente ao SUSE Linux Enterprise Desktop, visite a página de documentação específica do seu produto na Web em http://www.suse.com/doc/.

Se você estiver pesquisando mais informações relativas ao produto, também poderá consultar os seguintes sites:

Suporte Técnico do SUSE

Você encontra o Suporte Técnico do SUSE em http://www.suse.com/support/, em caso de dúvidas ou soluções para problemas técnicos.

Fóruns do SUSE

Há vários fóruns em que você pode participar de discussões sobre produtos do SUSE. Acesse http://forums.suse.com/ para obter uma lista.

Conversações sobre o SUSE

Uma comunidade online, que oferece artigos, dicas, Perguntas e Respostas e ferramentas gratuitas para fazer download: http://www.suse.com/communities/conversations/

Documentação do GNOME

A documentação para usuários, administradores e desenvolvedores do GNOME está disponível em http://library.gnome.org/.

O Projeto de Documentação do Linux

O TLDP (The Linux Documentation Project — O Projeto de Documentação do Linux) é administrado por uma equipe de voluntários que escrevem a documentação relacionada ao Linux (acesse http://www.tldp.org ↗). É provavelmente o recurso de documentação mais completo do Linux. O conjunto de documentos contém tutoriais para iniciantes, mas é direcionado principalmente a usuários experientes e administradores de sistema profissionais. O TLDP publica HOWTOs (Como Fazer), FAQs e guias (manuais) sob uma licença livre. Partes da documentação do TLDP também estão disponíveis no SUSE Linux Enterprise Desktop

Você também pode experimentar mecanismos de busca para fins gerais. Por exemplo, use os termos de pesquisa `ajuda Linux CD-RW` ou `problema de conversão de arquivos OpenOffice` se tiver problemas com a gravação de CDs ou a conversão de arquivos do LibreOffice.

30 Problemas comuns e suas soluções

Este capítulo descreve uma gama de problemas em potencial e suas soluções. Mesmo se a sua situação não esteja listada aqui com precisão, poderá haver alguma semelhante que ofereça dicas para a solução do seu problema.

30.1 Localizando e reunindo informações

O Linux reporta os dados de forma bastante detalhada. Há vários lugares para você pesquisar caso tenha problemas com seu sistema, sendo que a maioria é padrão para sistemas Linux em geral, e alguns relevantes aos sistemas SUSE Linux Enterprise Desktop. É possível ver a maioria dos arquivos de registro com o YaST (*Diversos* › *Registro de Inicialização*).

O YaST permite coletar todas as informações do sistema necessárias à equipe de suporte. Use *Outros* › *Suporte* e selecione a categoria do problema. Quando todas as informações forem reunidas, anexe-as à sua solicitação de suporte.

Veja a seguir uma lista dos arquivos de registro verificados com mais frequência com a descrição de seus objetivos principais. Os caminhos contendo `~` referem-se ao diretório pessoal do usuário atual.

TABELA 30.1 ARQUIVOS DE REGISTRO

Arquivo de registro	Descrição
`~/.xsession-errors`	Mensagens de aplicativos de área de trabalho atualmente em execução.
`/var/log/apparmor/`	Arquivos de registro do AppArmor, consulte a *Book* “Security Guide” para obter informações detalhadas.
`/var/log/audit/audit.log`	Arquivo de registro do Audit para monitorar qualquer acesso a arquivos, diretórios ou recursos do seu sistema, bem como rastrear as chamadas do sistema. Consulte a *Book* “Security Guide” para obter as informações detalhadas.

Arquivo de registro	Descrição
`/var/log/mail.*`	Mensagens do sistema de correio.
`/var/log/NetworkManager`	Arquivo de registro do NetworkManager para coleta de problemas de conectividade da rede
`/var/log/samba/`	Diretório contendo mensagens do registro de cliente e servidor do Samba.
`/var/log/warn`	Todas as mensagens do kernel e do daemon do registro do sistema com o nível “warning” ou superior.
`/var/log/wtmp`	Arquivo binário contendo registros de login de usuário para a sessão da máquina atual. Exiba-o com **`last`**.
`/var/log/Xorg.*.log`	Vários arquivos de registro de inicialização e tempo de execução do X Window System. São úteis para depurar inicializações malsucedidas do X.
`/var/log/YaST2/`	Diretório contendo ações do YaST e seus resultados.
`/var/log/zypper.log`	Arquivo de registro do Zypper.

Além dos arquivos de registro, a sua máquina também lhe fornece informações sobre o sistema em execução. Consulte a *Tabela 30.2: Informações do sistema no sistema de arquivos* `/proc`.

TABELA 30.2 INFORMAÇÕES DO SISTEMA NO SISTEMA DE ARQUIVOS `/proc`

Arquivo	Descrição
`/proc/cpuinfo`	Contém informações do processador, incluindo o seu tipo, marca, modelo e desempenho.

Arquivo	Descrição
`/proc/dma`	Mostra quais canais DMA estão sendo usados no momento.
`/proc/interrupts`	Mostra quais interrupções estão em uso e quantas de cada foram usadas.
`/proc/iomem`	Exibe o status da memória de E/S (entrada/saída).
`/proc/ioports`	Mostra quais portas de E/S estão em uso no momento.
`/proc/meminfo`	Exibe o status da memória.
`/proc/modules`	Exibe os módulos individuais.
`/proc/mounts`	Exibe os dispositivos montados no momento.
`/proc/partitions`	Mostra o particionamento de todos os discos rígidos.
`/proc/version`	Exibe a versão atual do Linux.

Além do sistema de arquivos `/proc`, o kernel do Linux exporta informações com o módulo `sysfs`, um sistema de arquivos na memória. Esse módulo representa objetos Kernel, seus atributos e relacionamentos. Para obter mais informações sobre o `sysfs`, consulte o contexto de udev no *Capítulo 17, Gerenciamento dinâmico de dispositivos do Kernel com* `udev`. A *Tabela 30.3* contém uma visão geral dos diretórios mais comuns em `/sys`.

TABELA 30.3 INFORMAÇÕES DO SISTEMA NO SISTEMA DE ARQUIVOS `/sys`

Arquivo	Descrição
`/sys/block`	Contém subdiretórios para cada dispositivo de bloco descoberto no sistema. Geralmente, esses dispositivos são de tipo de disco.
`/sys/bus`	Contém subdiretórios para cada tipo de barramento físico.

Arquivo	Descrição
`/sys/class`	Contém subdiretórios agrupados como tipos funcionais de dispositivos (como gráficos, de rede, de impressora etc.)
`/sys/device`	Contém a hierarquia global de dispositivos.

O Linux vem com várias ferramentas para monitoramento e análise do sistema. Consulte o *Book "System Analysis and Tuning Guide" 2 "System Monitoring Utilities"* para obter uma seleção das mais importantes usadas em diagnósticos de sistema.

Cada um dos seguintes cenários começa com um cabeçalho que descreve o problema, seguido de um ou dois parágrafos apresentando sugestões para solução, referências disponíveis para consultar soluções mais detalhadas e referências cruzadas para outros cenários relacionados.

30.2 Problemas de instalação

Problemas de instalação são situações que ocorrem quando a máquina falha na instalação. Ela pode falhar inteiramente ou talvez não consiga iniciar o instalador gráfico. Esta seção destaca alguns dos problemas típicos que você pode encontrar e oferece soluções ou alternativas possíveis para esses tipos de situações.

30.2.1 Verificação de mídia

Se você tiver qualquer problema ao usar a mídia de instalação do SUSE Linux Enterprise Desktop, verifique a integridade da mídia. Inicialize da mídia e escolha *Verificar a Mídia de Instalação* no menu de boot. No sistema em execução, inicie o YaST e escolha *Software* › *Verificação de Mídia*. Para verificar o meio do SUSE Linux Enterprise Desktop, insira-o na unidade e clique em *Iniciar Verificação* na tela *Verificação de Mídia* do YaST. Isso pode levar alguns minutos. Se forem detectados erros, não use esta mídia para instalação. Problemas de mídia podem ocorrer com o meio que você mesmo gravou. A gravação de mídia a baixa velocidade (4x) ajuda a evitar problemas.

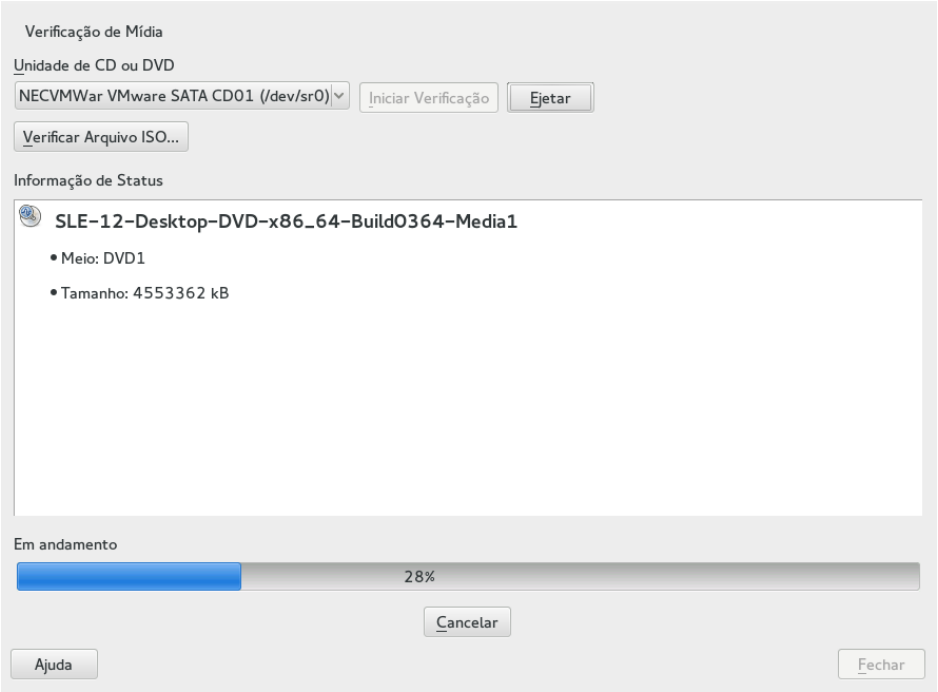


FIGURA 30.1 VERIFICAÇÃO DE MÍDIA

30.2.2 Nenhuma unidade de DVD inicializável disponível

Se o seu computador não contém uma unidade de DVD-ROM inicializável ou se a que você tem não é suportada pelo Linux, há várias opções para instalar sua máquina sem uma unidade de DVD interna:

Usando um dispositivo de inicialização externo

Se for suportado pelo BIOS e pelo kernel de instalação, inicialize pelas unidades de DVD externas ou dispositivos de armazenamento USB. Consulte a para obter instruções de como criar um dispositivo de armazenamento USB inicializável.

Inicialização de rede via PXE

Se a máquina não tiver uma unidade de DVD, mas oferecer uma conexão Ethernet ativa, execute a instalação completamente baseada em rede. Consulte a *Book* “Deployment Guide” *11 “Remote Installation”11.1.3 “Remote Installation via VNC—PXE Boot and Wake on LAN”* e a *Book* “Deployment Guide” *11 “Remote Installation”11.1.6 “Remote Installation via SSH—PXE Boot and Wake on LAN”* para obter os detalhes.

30.2.2.1 Dispositivos de inicialização externos

O Linux suporta a maioria das unidades de DVD existentes. Mesmo que o sistema não tenha uma unidade de DVD, ainda será possível usar uma unidade de DVD externa, conectada por USB, FireWire ou SCSI, para inicializar o sistema. Isso depende principalmente da interação entre o BIOS e o hardware usado. Algumas vezes uma atualização do BIOS pode ajudar se você tiver problemas.

Ao instalar de um Live CD, também é possível criar um "disco flash Live USB" do qual inicializar.

30.2.3 Falha na inicialização da mídia de instalação

Um motivo possível para a máquina não inicializar a mídia de instalação é uma configuração incorreta de sequência de boot no BIOS. A sequência de boot do BIOS deve ter uma unidade de DVD definida como a primeira entrada de boot. De outra forma, a máquina tentaria inicializar de outro meio, normalmente o disco rígido. Você encontra instruções de como mudar a sequência de boot do BIOS na documentação que acompanha sua placa-mãe, ou nos parágrafos a seguir.

O BIOS é o software que habilita as funções mais básicas de um computador. Fabricantes de placas-mãe fornecem um BIOS especificamente fabricado para o hardware. Normalmente, a configuração do BIOS só pode ser acessada em um momento específico: quando a máquina está inicializando. Durante a fase de inicialização, a máquina executa vários testes de diagnóstico de hardware. Um deles é uma verificação de memória, indicado por um contador de memória. Quando o contador aparecer, procure uma linha, geralmente abaixo dele ou em algum local na parte inferior, mencionando a tecla a ser pressionada para acessar a configuração do BIOS. Geralmente, a tecla a ser pressionada é `Del`, `F1` ou `Esc`. Pressione esta tecla até que a tela de configuração do BIOS seja exibida.

PROCEDIMENTO 30.1 MUDANDO A SEQUÊNCIA DE INICIALIZAÇÃO DO BIOS

1. Digite o BIOS usando a tecla apropriada conforme anunciada pelas rotinas de inicialização e espere até que a tela do BIOS seja exibida.

2. Para mudar a sequência de inicialização em um AWARD BIOS, procure a entrada *BIOS FEATURES SETUP*. Outros fabricantes talvez tenham um nome diferente para isso, como *ADVANCED CMOS SETUP*. Quando encontrar a entrada, selecione-a e confirme com `Enter`.

3. Na tela exibida, procure uma subentrada denominada *BOOT SEQUENCE* ou *BOOT ORDER*. Modifique as configurações pressionando PgUp ou PgDown até a unidade de DVD aparecer primeiro na lista.

4. Saia da tela de configuração do BIOS pressionando Esc. Para gravar as mudanças, selecione *SAVE & EXIT SETUP* ou pressione F10. Para confirmar que as configurações devem ser gravadas, pressione Y.

PROCEDIMENTO 30.2 MUDANDO A SEQUÊNCIA DE INICIALIZAÇÃO EM UM SCSI BIOS (ADAPTADOR DE HOST ADAPTEC)

1. Abra a configuração pressionando Ctrl–A.

2. Selecione *Utilitários de Disco*. Os componentes de hardware conectados agora são exibidos. Anote o ID do SCSI da sua unidade de DVD.

3. Saia do menu com Esc.

4. Abra *Definir Configurações do Adaptador*. Em *Opções Adicionais*, selecione *Opções do Dispositivo de Inicialização* e pressione Enter.

5. Digite o ID da unidade de DVD e pressione Enter novamente.

6. Pressione Esc duas vezes para retornar à tela de inicialização do BIOS do SCSI.

7. Saia dessa tela e confirme com *Sim* para inicializar o computador.

Independentemente do idioma e do layout do teclado que a instalação final usará, a maioria das configurações de BIOS usa o layout de teclado dos EUA, conforme mostrado na figura a seguir:

FIGURA 30.2 LAYOUT DO TECLADO DOS EUA

30.2.4 Falha na inicialização

Alguns tipos de hardware, principalmente os muito antigos ou muito recentes, falham na instalação. Em muitos casos, isso pode ocorrer devido à ausência de suporte para esse tipo de hardware no kernel de instalação ou devido a alguma funcionalidade incluída no kernel, como a ACPI, que ainda causa problemas em alguns hardwares.

Se o seu sistema falhar na instalação usando o modo de *instalação* padrão da primeira tela de boot da instalação, tente o seguinte:

1. Com o DVD ainda na unidade, reinicialize a máquina com Ctrl–Alt–Del ou usando o botão de reinicialização do hardware.
2. Quando a tela de boot for exibida, pressione F5, use as teclas de seta do teclado para navegar até *Sem ACPI* e pressione Enter para iniciar o processo de boot e instalação. Essa opção desabilita o suporte para as técnicas de gerenciamento de energia da ACPI.
3. Prossiga com a instalação conforme descrito no *Book “Deployment Guide” 3 “Installation with YaST”*.

Se isso falhar, proceda como acima, mas escolha *Configurações Seguras*. Essa opção desabilita o suporte de ACPI e DMA. A maioria dos hardwares inicializará com essa opção.

Se ambas as opções falharem, use o prompt das opções de boot para transmitir quaisquer parâmetros adicionais necessários para suportar esse tipo de hardware no kernel de instalação. Para obter mais informações sobre os parâmetros disponíveis como opções de boot, consulte a documentação do kernel localizada em `/usr/src/linux/Documentation/kernel-parameters.txt`.

Dica: obtendo documentação do kernel

Instale o pacote `kernel-source` para exibir a documentação do kernel.

Há vários outros parâmetros de kernel relacionados à ACPI que podem ser digitados no prompt de inicialização antes da inicialização para a instalação:

`acpi=off`

Esse parâmetro desabilita o subsistema completo da ACPI no seu computador. Isso poderá ser útil se o computador não puder lidar com a ACPI de modo algum ou se você achar que a ACPI no computador causa problemas.

`acpi=force`

Sempre habilite a ACPI mesmo que o computador tenha um BIOS antigo anterior ao ano 2000. Esse parâmetro também habilitará a ACPI se ele estiver definido além de `acpi=off`.

`acpi=noirq`

Não use a ACPI para roteamento de IRQ.

`acpi=ht`

Execute somente ACPI o suficiente para habilitar hyper-threading.

`acpi=strict`

Tenha menos tolerância com plataformas que não sejam estritamente compatíveis com a especificação ACPI.

`pci=noacpi`

Desabilita o roteamento de IRQ de PCI do novo sistema da ACPI.

`pnpacpi=off`

Essa opção serve para problemas de porta serial ou paralela quando a configuração do BIOS contiver interrupções ou portas incorretas.

`notsc`

Desabilita o contador da marcação de horário. Essa opção pode ser usada para solucionar problemas de tempo nos seus sistemas. Trata-se de um recurso recente, por isso, se você perceber regressões na sua máquina, especialmente relativas a horário ou mesmo um travamento total, vale a pena tentar essa opção.

`nohz=off`

Desabilita o recurso nohz. Se a sua máquina trava, essa opção pode ajudar. Caso contrário, ela não tem utilidade.

Após determinar a combinação correta de parâmetros, o YaST os grava automaticamente na configuração do carregador de boot para verificar se o sistema inicializará de forma correta na próxima vez.

Se erros inexplicáveis ocorrerem quando o kernel estiver carregado ou durante a instalação, selecione *Teste de Memória* no menu de inicialização para verificar a memória. Se *Teste de Memória* retornar um erro, geralmente será um erro de hardware.

30.2.5 Falha na inicialização do instalador gráfico

Depois que você insere o meio na unidade e reinicializa a máquina, a tela de instalação é exibida, mas depois que a opção *Instalação* é selecionada, o instalador gráfico não inicializa.

Há várias maneiras de lidar com essa situação:

- Tente selecionar outra resolução de tela para as caixas de diálogo de instalação.
- Selecione *Modo de Texto* para a instalação.
- Faça uma instalação remota através de VNC usando o instalador gráfico.

PROCEDIMENTO 30.3 MUDAR A RESOLUÇÃO DE TELA PARA INSTALAÇÃO

1. Inicialize para a instalação.
2. Pressione F3 para abrir um menu do qual selecionar uma resolução mais baixa para fins de instalação.
3. Selecione *Instalação* e prossiga com a instalação conforme descrito no *Book* “Deployment Guide” *3 “Installation with YaST”*.

PROCEDIMENTO 30.4 INSTALAÇÃO EM MODO DE TEXTO

1. Inicialize para a instalação.
2. Pressione F3 e selecione *Modo de Texto*.
3. Selecione *Instalação* e prossiga com a instalação conforme descrito no *Book* “Deployment Guide” *3 “Installation with YaST”*.

PROCEDIMENTO 30.5 INSTALAÇÃO VNC

1. Inicialize para a instalação.
2. Insira o texto a seguir no prompt de opções de boot:

   ```
   vnc=1 vncpassword=some_password
   ```

   Substitua *senha* pela senha a ser usada para a instalação do VNC.
3. Selecione *Instalação* e pressione Enter para iniciar a instalação.

Em vez de iniciar com a rotina de instalação gráfica, o sistema continua em execução no modo de texto, depois trava, exibindo uma mensagem que contém o endereço IP e o número de porta com que o instalador pode ser acessado por uma interface de browser ou um aplicativo viewer do VNC.

4. Se estiver usando um browser para acessar o instalador, inicie o browser e digite as informações de endereço fornecidas pelas rotinas de instalação na futura máquina do SUSE Linux Enterprise Desktop e pressione `Enter`:

```
http://ip_address_of_machine:5801
```

Uma caixa de diálogo é aberta na janela do browser solicitando a senha VNC. Insira-a e continue com a instalação conforme descrito no *Book "Deployment Guide" 3 "Installation with YaST"*.

Importante: Suporte a vÃ¡rias plataformas

A instalação através de VNC funciona com qualquer navegador em qualquer sistema operacional, desde que o suporte Java esteja habilitado.

Forneça o endereço IP e a senha do seu viewer do VNC quando solicitado. Uma janela é aberta, exibindo as caixas de diálogo de instalação. Prossiga com a instalação como de costume.

30.2.6 Apenas a tela de boot simples é aberta

Você inseriu o meio na unidade, as rotinas do BIOS foram encerradas, mas o sistema não inicia com a tela de boot gráfica. Em vez disso, ele inicia uma interface baseada em texto bastante simples. Isso pode acontecer em qualquer máquina que não forneça memória gráfica suficiente para renderizar uma tela de boot gráfica.

Embora a tela de boot de texto tenha aparência simples, ela fornece praticamente a mesma funcionalidade que a gráfica:

Opções de Boot

Diferentemente da interface gráfica, as diversas opções de boot não podem ser selecionadas usando as teclas de cursor do teclado. O menu de inicialização da tela de boot em modo de texto oferece algumas palavras-chave no prompt de inicialização. Essas palavras-chave são mapeadas para as opções oferecidas na versão gráfica. Insira sua escolha e pressione `Enter` para iniciar o processo de boot.

Opções de Boot Personalizadas

Após selecionar uma opção de boot, insira a palavra-chave apropriada no prompt de boot ou insira algumas opções de boot personalizadas conforme descrito na *Seção 30.2.4, "Falha na inicialização"*. Para iniciar o processo de instalação, pressione `Enter`.

Resoluções de tela

Use as teclas F para determinar a resolução de tela para a instalação. Se você precisa inicializar no modo de texto, escolha `F3`.

30.3 Problemas de boot

Problemas de boot são situações em que o sistema não é inicializado apropriadamente (não é inicializado no destino e na tela de login esperados).

30.3.1 Falha ao carregar o carregador de boot GRUB 2

Se o hardware estiver funcionando de forma adequada, é possível que o carregador de boot esteja corrompido e que o Linux não possa ser iniciado na máquina. Neste caso, é necessário consertar o carregador de boot. Para isso, é necessário iniciar o Sistema de Recuperação conforme descrito na *Seção 30.6.2, "Usando o sistema de recuperação"* e seguir as instruções na *Seção 30.6.2.4, "Modificando e reinstalando o carregador de boot"*.

Outros motivos para a máquina não inicializar podem estar relacionadas ao BIOS:

Configurações do BIOS

Verifique o BIOS para obter referências sobre o disco rígido. O GRUB 2 talvez não seja iniciado se o próprio disco rígido não for encontrado com as configurações atuais do BIOS.

Ordem de inicialização do BIOS

Verifique se a ordem de inicialização do sistema inclui o disco rígido. Se a opção do disco rígido não tiver sido habilitada, o sistema talvez seja instalado de forma adequada, mas não seja inicializado quando o acesso ao disco rígido for necessário.

30.3.2 Não é exibido nenhum prompt nem tela de login

Isso costuma ocorrer após uma falha de atualização do kernel e é conhecido como *pânico do kernel* devido ao tipo de erro do console do sistema que às vezes se verifica no estágio final do processo. Se a máquina realmente tiver sido reinicializada após uma atualização de software, o objetivo imediato é reinicializá-la usando a versão antiga e segura do kernel do Linux e os arquivos associados. Isso pode ser feito na tela do carregador de boot GRUB 2 durante o processo de boot da seguinte forma:

1. Reinicialize o computador usando o botão de reinicialização ou desligue-o e ligue-o novamente.
2. Quando a tela de boot do GRUB 2 for exibida, selecione a entrada *Opções Avançadas* e escolha o kernel anterior no menu. A máquina será inicializada com a versão anterior do kernel e seus arquivos associados.
3. Após a conclusão do processo de boot, remova o kernel recém-instalado e, se necessário, defina a entrada de boot padrão como o kernel antigo usando o módulo *Carregador de Boot* do YaST. Para obter mais informações, consulte a *Seção 13.3, "Configurando o carregador de boot com o YaST"*. No entanto, isso talvez não seja necessário porque as ferramentas automatizadas de atualização normalmente o modificam durante o processo de rollback.
4. Reinicializar.

Se isso não resolver o problema, inicialize o computador usando a mídia de instalação. Após a inicialização da máquina, prossiga com o *Passo 3*.

30.3.3 Não há login gráfico

Se a máquina ligar, mas não for inicializada no gerenciador de login gráfico, evite problemas com a opção de destino padrão do systemd ou com a configuração do X Window System. Para verificar o destino padrão atual do systemd, execute o comando **`sudo systemctl get-default`**.

Se o valor retornado *não* for `graphical.target`, execute o comando **`sudo systemctl isolate graphical.target`**. Se a tela gráfica de login for iniciada, efetue login e inicie o *YaST › Sistema › Services Manager* (Gerenciador de Serviços) e defina o *Default System Target* (Destino do Sistema Padrão) como *Graphical Interface* (Interface Gráfica). De agora em diante, o sistema deverá ser inicializado na tela gráfica de login.

Se a tela gráfica de login não for iniciada mesmo depois de ter sido inicializada ou alternada para o destino gráfico, a área de trabalho ou o software do X Window provavelmente foi mal configurado ou estava corrompido. Examine os arquivos de registro em `/var/log/Xorg.*.log` para obter mensagens detalhadas do servidor X enquanto ele tenta iniciar. Se a área de trabalho falhar durante a inicialização, talvez ela registre mensagens de erro no diário do sistema que possam ser consultadas com o comando **`journalctl`** (leia o *Capítulo 12, `journalctl`: consultar o diário do `systemd`* para obter mais informações). Se essas mensagens de erro sugerirem um problema de configuração no servidor X, tente corrigi-lo. Se o sistema gráfico ainda não aparecer, reinstale a área de trabalho gráfica.

30.3.4 Não é possível montar a partição Btrfs raiz

Se uma partição `btrfs` raiz for corrompida, tente as seguintes opções:

- Monte a partição com a opção `-o recovery`.
- Se isso não funcionar, execute **`btrfs-zero-log`** na partição raiz.

30.4 Problemas de login

Problemas de login são aqueles em que sua máquina, de fato, é inicializada na tela de boas-vindas ou no prompt de login esperados, mas se recusa a aceitar o nome de usuário e a senha ou os aceita mas não se comporta apropriadamente (não inicia a área de trabalho gráfica, produz erros, passa para uma linha de comando, etc.).

30.4.1 Falha nas combinações de nome de usuário e senha válidas

Isso geralmente ocorre quando o sistema está configurado para usar autenticação de rede ou serviços de diretório e, por alguma razão, não é capaz de recuperar resultados de seus servidores configurados. O usuário `root`, como o único usuário local, é o único que ainda pode efetuar login nessas máquinas. A seguir estão alguns motivos comuns para uma máquina parecer funcional, mas não conseguir processar logins corretamente:

- A rede não está funcionando. Para obter mais instruções sobre isso, consulte a *Seção 30.5, "Problemas de rede"*.
- O DNS não está funcionando no momento (o que impede o GNOME de trabalhar e o sistema de efetuar solicitações válidas a servidores seguros). Uma indicação de que esse é o caso é que a máquina leva muito tempo para responder a qualquer ação. Há mais informações a respeito desse tópico na *Seção 30.5, "Problemas de rede"*.
- Se o sistema estiver configurado para usar Kerberos, o horário local do sistema poderá ter ultrapassado a variação aceita com o horário do servidor Kerberos (geralmente 300 segundos). Se o NTP (protocolo de horário de rede) não estiver funcionando de forma adequada ou os servidores NTP locais não estiverem funcionando, a autenticação do Kerberos não funcionará pois depende da sincronização comum do relógio na rede.
- A configuração de autenticação do sistema está definida incorretamente. Verifique se há erros de digitação ou ordem incorreta de diretivas nos arquivos de configuração PAM envolvidos. Para obter informações adicionais sobre o PAM e a sintaxe dos arquivos de configuração envolvidos, consulte o *Book "Security Guide" 2 "Authentication with PAM"*.
- A partição pessoal está criptografada. Há mais informações a respeito desse tópico na *Seção 30.4.3, "Falha de login na partição pessoal criptografada"*.

Em todos os casos que não envolvem problemas de rede externos, a solução é reinicializar o sistema em um modo de usuário único e reparar a configuração antes de inicializar novamente no modo de operação e tentar efetuar login novamente. Para inicializar no modo de usuário único:

1. Reinicialize o sistema. A tela de boot é exibida e apresenta um prompt.
2. Pressione Esc para sair da splash screen e entrar no menu baseado em texto do GRUB 2.

3. Pressione B para entrar no editor do GRUB 2.
4. Adicione o seguinte parâmetro à linha com os parâmetros do Kernel:

```
systemd.unit=rescue.target
```

5. Pressione F10.
6. Digite o nome de usuário e a senha de `root`.
7. Faça as mudanças necessárias.
8. Inicialize no modo completo multiusuário e de rede inserindo **`systemctl isolate graphical.target`** na linha de comando.

30.4.2 Nome de usuário e senha não aceitos

Esse é o um dos problemas mais comuns que os usuários podem encontrar, pois há vários motivos pelos quais isso pode ocorrer. Dependendo de você usar gerenciamento e autenticação de usuário local ou autenticação em rede, as falhas de login ocorrem por motivos diferentes.

O gerenciamento de usuário local pode falhar pelos seguintes motivos:

- O usuário pode ter digitado a senha errada.
- O diretório pessoal do usuário que contém arquivos de configuração da área de trabalho está corrompido ou protegido contra gravação.
- Talvez haja problemas com o sistema X Window ao autenticar esse usuário específico, especialmente se o diretório pessoal do usuário tiver sido usado com outra distribuição do Linux antes da instalação da atual.

Para encontrar o motivo de uma falha de login local, proceda da seguinte maneira:

1. Verifique se o usuário memorizou a senha corretamente antes de começar a depurar todo o mecanismo de autenticação. Se o usuário não se lembrar da senha corretamente, use o módulo Gerenciamento de Usuário do YaST para mudar a senha dele. Fique atento à tecla Caps Lock e libere-a, se necessário.
2. Efetue login como `root` e consulte o diário do sistema com o comando **`journalctl -e`** para verificar se há mensagens de erro do processo de login e do PAM.

3. Tente efetuar login de um console (usando Ctrl–Alt–F1). Se esse procedimento for bem-sucedido, não será responsabilidade do PAM, pois é possível autenticar o usuário nessa máquina. Tente localizar quaisquer problemas com o X Window System ou com a área de trabalho do GNOME. Para obter mais informações, consulte a *Seção 30.4.4, "Login bem-sucedido, mas há falha na área de trabalho do GNOME"*.

4. Se o diretório pessoal do usuário foi usado com outra distribuição Linux, remova o arquivo `Xauthority` no diretório do usuário. Use um login de console por meio de Ctrl–Alt–F1 e execute o comando **`rm .Xauthority`** como esse usuário. Isso deve eliminar problemas de autenticação X para o usuário. Tente o login gráfico novamente.

5. Se não for possível iniciar a área de trabalho devido a arquivos de configuração corrompidos, continue na *Seção 30.4.4, "Login bem-sucedido, mas há falha na área de trabalho do GNOME"*.

Veja a seguir alguns motivos comuns pelos quais a autenticação em rede de um usuário específico pode falhar em uma máquina específica:

- O usuário pode ter digitado a senha errada.
- O nome de usuário existe nos arquivos de autenticação locais da máquina e também são fornecidos por um sistema de autenticação de rede, gerando conflitos.
- O diretório pessoal existe mas está corrompido ou não disponível. Talvez ele esteja protegido contra gravação ou está em um servidor inacessível no momento.
- O usuário não tem permissão para efetuar login neste host específico no sistema de autenticação.
- A máquina mudou os nomes de host, por algum motivo, e o usuário não tem permissão para efetuar login nesse host.
- A máquina não pode acessar o servidor de diretório ou o servidor de autenticação que contém as informações do usuário.
- Talvez haja problemas com o sistema X Window ao autenticar esse usuário específico, especialmente se o diretório pessoal do usuário tiver sido usado com outra distribuição do Linux antes da instalação da atual.

Para localizar a causa das falhas de login com a autenticação de rede, proceda da seguinte maneira:

1. Verifique se o usuário memorizou a senha corretamente antes de começar a depurar todo o mecanismo de autenticação.
2. Determine o servidor de diretórios usado pela máquina para autenticação e verifique se ele está funcionando e se comunicando corretamente com as outras máquinas.
3. Determine se o nome e a senha do usuário funcionam em outras máquinas para verificar se os dados de autenticação existem e são distribuídos apropriadamente.
4. Verifique se outro usuário pode efetuar login na máquina com comportamento incorreto. Se outro usuário ou o usuário `root` puder efetuar login sem dificuldade, efetue login e examine o diário do sistema com o comando **`journalctl -e`** > arquivo. Localize as marcações de horário que correspondem às tentativas de login e determine se o PAM produziu alguma mensagem de erro.
5. Tente efetuar login de um console (usando Ctrl–Alt–F1). Se der certo, o problema não é do PAM ou do servidor de diretórios no qual o diretório pessoal do usuário está hospedado, pois é possível autenticar o usuário nessa máquina. Tente localizar quaisquer problemas com o X Window System ou com a área de trabalho do GNOME. Para obter mais informações, consulte a *Seção 30.4.4, "Login bem-sucedido, mas há falha na área de trabalho do GNOME"*.
6. Se o diretório pessoal do usuário foi usado com outra distribuição Linux, remova o arquivo `Xauthority` no diretório do usuário. Use um login de console por meio de Ctrl–Alt–F1 e execute o comando **`rm .Xauthority`** como esse usuário. Isso deve eliminar problemas de autenticação X para o usuário. Tente o login gráfico novamente.
7. Se não for possível iniciar a área de trabalho devido a arquivos de configuração corrompidos, continue na *Seção 30.4.4, "Login bem-sucedido, mas há falha na área de trabalho do GNOME"*.

30.4.3 Falha de login na partição pessoal criptografada

Recomenda-se o uso de uma partição pessoal criptografada para laptops. Se você não puder efetuar login no seu laptop, o motivo geralmente é simples: a sua partição pode não estar desbloqueada.

Durante a inicialização, é necessário digitar a frase secreta para desbloquear a partição criptografada. Se você não a digitar, o processo de boot continuará, deixando a partição bloqueada.

Para desbloquear a partição criptografada, faça o seguinte:

1. Passe para o console de texto com Ctrl–Alt–F1.
2. Torne-se `root`.
3. Reinicie o processo de desbloqueio novamente com:

```
systemctl restart home.mount
```

4. Digite sua frase secreta para desbloquear a partição criptografada.
5. Saia do console de texto e volte para a tela de login com Alt–F7.
6. Efetue login como de costume.

30.4.4 Login bem-sucedido, mas há falha na área de trabalho do GNOME

Se esse for o caso, provavelmente os seus arquivos de configuração do GNOME se corromperam. Alguns sintomas podem incluir falha de funcionamento do teclado, a geometria da tela distorcida ou até mesmo a tela exibida como um campo cinza vazio. A distinção importante é que se outro usuário efetuar login, a máquina funcionará normalmente. Provavelmente o problema possa ser corrigido rapidamente com a transferência do diretório de configuração do GNOME do usuário para um novo local, o que faz a área de trabalho do GNOME inicializar um novo. Embora o usuário seja forçado a reconfigurar o GNOME, nenhum dado é perdido.

1. Alterne para um console de texto pressionando Ctrl–Alt–F1.
2. Efetue login com o seu nome de usuário.
3. Mova os diretórios de configuração do GNOME do usuário para um local temporário:

```
mv .gconf  .gconf-ORIG-RECOVER
mv .gnome2 .gnome2-ORIG-RECOVER
```

4. Efetue logout.

5. Efetue login novamente, mas não execute nenhum aplicativo.

6. Recupere seus dados individuais de configuração de aplicativo (inclusive os dados de cliente de e-mail do Evolution) copiando o diretório `~/gconf-ORIG-RECOVER/apps/` de volta para o novo diretório `~/.gconf` da seguinte maneira:

   ```
   cp -a .gconf-ORIG-RECOVER/apps .gconf/
   ```

   Se isso causar os problemas de login, tente recuperar somente os dados de aplicativo críticos e reconfigure o restante dos aplicativos.

30.5 Problemas de rede

Quaisquer problemas do seu sistema podem estar relacionados à rede, mesmo que inicialmente não transmitam essa impressão. Por exemplo, o motivo para um sistema não permitir o login de usuários pode ser algum tipo de problema de rede. Esta seção apresenta uma lista de verificação simples que você pode aplicar para identificar a causa de qualquer problema de rede encontrado.

PROCEDIMENTO 30.6 COMO IDENTIFICAR PROBLEMAS DE REDE

Ao verificar a conexão de rede da sua máquina, proceda da seguinte maneira:

1. Se você usa uma conexão Ethernet, verifique o hardware primeiro. Verifique se o cabo de rede está acoplado corretamente no computador e no roteador (ou hub etc.). As luzes de controle próximas ao seu conector Ethernet normalmente estão ativas.
   Se a conexão falhar, verifique se o cabo de rede funciona com outra máquina. Se funcionar, a placa de rede será a causa da falha. Se houver hubs ou switches incluídos na configuração da sua rede, eles também podem estar com defeito.

2. Se estiver usando uma conexão sem fio, verifique se o link sem fio pode ser estabelecido por outras máquinas. Caso contrário, contate o administrador da rede wireless.

3. Após verificar sua conectividade de rede básica, tente descobrir qual serviço não está respondendo. Reúna as informações de endereço de todos os servidores de rede necessários na configuração. Procure-os no módulo YaST apropriado ou consulte o administrador de sistema. A lista a seguir fornece alguns dos servidores de rede típicos envolvidos em uma configuração junto com os sintomas de uma falha.

DNS (Serviço de Nomes)

Um serviço de nomes inoperante ou defeituoso afeta a funcionalidade da rede de várias maneiras. Se a máquina local depender de quaisquer servidores de rede para autenticação e esses servidores não forem encontrados devido a problemas de resolução de nome, os usuários não poderão nem efetuar login. As máquinas na rede gerenciadas por um servidor de nomes com defeito não podem “ver” umas às outras nem se comunicar.

NTP (Serviço de Horário)

Um serviço NTP defeituoso ou totalmente inoperante pode afetar a funcionalidade do servidor X e a autenticação Kerberos.

NFS (Serviço de Arquivos)

Se qualquer aplicativo precisar de dados armazenados em um diretório NFS montado, ele não conseguirá iniciar nem funcionar corretamente se esse serviço estiver inoperante ou mal configurado. No pior cenário possível, a configuração da área de trabalho pessoal de um usuário não será exibida se o seu diretório pessoal que contém o subdiretório `.gconf` não for encontrado por causa de um servidor NFS defeituoso.

Samba (Serviço de Arquivos)

Se qualquer aplicativo precisar de dados armazenados em um diretório de um servidor Samba defeituoso, ele não conseguirá iniciar ou funcionar corretamente.

NIS (Gerenciamento de Usuário)

Se o sistema SUSE Linux Enterprise Desktop usar um servidor NIS defeituoso para fornecer os dados de usuários, os usuários não poderão efetuar login na máquina.

LDAP (Gerenciamento de Usuário)

Se o sistema SUSE Linux Enterprise Desktop usar um servidor LDAP defeituoso para fornecer os dados de usuários, os usuários não poderão efetuar login na máquina.

Kerberos (Autenticação)

A autenticação não funcionará e o login em qualquer máquina falhará.

CUPS (Impressão de Rede)

Os usuários não conseguem imprimir.

4. Verifique se os servidores de rede estão em execução e se a configuração de rede permite estabelecer uma conexão:

Importante: Limitações

O procedimento de depuração descrito abaixo aplica-se somente a uma configuração simples de servidor/cliente de rede que não envolva roteamento interno. Supõe-se que o servidor e o cliente integrem a mesma sub-rede sem necessidade de roteamento adicional.

a. Use **`ping`** *`endereço IP`* **`ou`** *`nome de host`* (substitua *`nome de host`* pelo nome de host do servidor) para verificar se cada um deles está ativo e respondendo à rede. Se esse comando for bem-sucedido, ele informará que o host que você estava procurando está em execução e o serviço de nomes da rede está configurado corretamente.
   Se o ping falhar com `destination host unreachable`, o seu sistema ou o servidor desejado não está configurado de forma adequada ou está inoperante. Verifique se o sistema pode ser acessado com **`ping`** *`endereço IP`* **`ou`** *`nome_de_host`* de outra máquina. Se você obtiver êxito em acessar sua máquina de outra máquina, significará que o servidor não está sendo executado ou não está configurado corretamente.
   Se o ping falhar com `unknown host` (host desconhecido), o serviço de nomes não foi configurado corretamente ou o nome de host usado estava incorreto. Para obter mais verificações sobre esse assunto, consulte o *Passo 4.b*. Se o ping ainda falhar, significará que a placa de rede não está configurada de forma correta ou o hardware de rede está defeituoso.

b. Use **`host`** *`nome de host`* para verificar se o nome de host do servidor ao qual você está tentando se conectar foi apropriadamente convertido em um endereço IP e vice-versa. Se esse comando retornar o endereço IP do host, significará que o serviço de nomes está funcionando. Se houver falha nesse comando **`host`**, verifique todos os arquivos de configuração de rede relacionados à resolução de nomes e de endereços no seu host:

`/etc/resolv.conf`

Este arquivo é usado para controlar o domínio e o servidor de nomes que você está usando no momento. Ele pode ser modificado manualmente ou ajustado automaticamente pelo YaST ou DHCP. O ajuste automático é preferencial. Porém, verifique se o arquivo tem a estrutura a seguir e se todos os endereços de rede e nomes de domínio estão corretos:

```
search fully_qualified_domain_name
nameserver ipaddress_of_nameserver
```

Este arquivo pode conter mais de um endereço de servidor de nomes, mas pelo menos um deles deve estar correto para fornecer a resolução de nomes para o seu host. Se necessário, ajuste o arquivo usando o módulo Configurações de Rede do YaST (guia Nome de host/DNS).

Se a conexão de rede for gerenciada por DHCP, habilite o DHCP para mudar as informações de serviço de nomes e de nome de host selecionando *Trocar Nome de Host via DHCP* e *Atualizar Servidores de Nomes e Lista de Pesquisa via DHCP* no módulo DNS e Nome de Host do YaST.

`/etc/nsswitch.conf`

Este arquivo informa ao Linux onde procurar informações de serviço de nomes. Ele deve ter a seguinte aparência:

```
 ...
hosts: files dns
networks: files dns
...
```

A entrada `dns` é essencial. Ela informa ao Linux para usar um servidor de nomes externo. Normalmente, essas entradas são gerenciadas automaticamente pelo YaST, mas convém verificar.

Se todas as entradas relevantes no host estiverem corretas, deixe o seu administrador de sistema verificar a configuração do servidor DNS para obter as informações de zona corretas. Se você verificou se a configuração DNS do seu host e o servidor DNS estão corretos, continue verificando a configuração da rede e do dispositivo de rede.

c. Se o sistema não puder estabelecer uma conexão a um servidor de redes e você excluiu problemas de serviço de nomes da lista de possíveis responsáveis, verifique a configuração da placa de rede.
   Use o comando **`ip addr show`** *`dispositivo_de_rede`* para verificar se o dispositivo foi configurado apropriadamente. Verifique se o `endereço inet` com a máscara de rede (*`/máscara`*) está configurado corretamente. Um erro no endereço IP ou um bit ausente na máscara de rede inutilizam a configuração de rede. Se necessário, execute essa verificação no servidor também.

d. Se o hardware de rede e o serviço de nomes estiverem configurados de forma adequada e em execução, mas algumas conexões de rede externas ainda tiverem longos tempos de espera ou falharem inteiramente, use **`traceroute`** *`nome_completo_do_domínio`* (executado como `root`) para controlar a rota de rede tomada pelas solicitações. Esse comando lista qualquer gateway (hop) que uma solicitação da sua máquina transmitir no caminho ao seu destino. Ele lista o tempo de resposta de cada hop e se esse hop é acessível. Use uma combinação de traceroute e ping para identificar o responsável e informar aos administradores.

Após identificar a causa do problema de rede, você poderá resolvê-lo (se o problema estiver na sua máquina) ou informar os administradores de sistema da rede sobre suas descobertas para que eles possam reconfigurar os serviços ou reparar os sistemas necessários.

30.5.1 Problemas no NetworkManager

Se você tiver problema com a conectividade da rede, restrinja-a conforme descrito no *Procedimento 30.6, "Como identificar problemas de rede"*. Se tudo indicar que a culpa é do NetworkManager, faça o seguinte para obter os registros com dicas sobre o motivo da falha do NetworkManager:

1. Abra um shell e efetue login como `root`.
2. Reinicie o NetworkManager:

```
systemctl restart Network.Manager.service
```

3. Abra uma página da Web, por exemplo http://www.opensuse.org, como usuário normal para ver se você consegue se conectar.
4. Colete as informações sobre o estado do NetworkManager em `/var/log/NetworkManager`.

Para obter maiores informações sobre o NetworkManager, consulte o *Capítulo 22, Usando o NetworkManager*.

30.6 Problemas de dados

Problemas de dados ocorrem quando a máquina pode ou não inicializar corretamente, mas em ambos os casos, está claro que há dados corrompidos no sistema e que o sistema precisa ser recuperado. Essas situações exigem um backup dos seus dados críticos, permitindo que você recupere o estado anterior à falha do sistema. O SUSE Linux Enterprise Desktop oferece módulos do YaST dedicados para backup e restauração do sistema e um sistema de recuperação que pode ser usado para recuperar um sistema corrompido externamente.

30.6.1 Gerenciando imagens de partição

Às vezes é necessário fazer um backup de uma partição inteira ou até do disco rígido. O Linux possui a ferramenta **`dd`**, capaz de criar uma cópia exata do seu disco. Combinada ao **`gzip`**, faz você economizar espaço.

PROCEDIMENTO 30.7 FAZENDO BACKUP E RESTAURANDO DISCOS RÍGIDOS

1. Inicie um Shell como usuário `root`.
2. Selecione o seu dispositivo de origem. Normalmente, ele assemelha-se a `/dev/sda` (com a etiqueta *`SOURCE`*).
3. Indique onde deseja armazenar sua imagem (com a etiqueta *`CAMINHO_BACKUP`*). Esse local deverá ser diferente do dispositivo de origem. Em outras palavras: se você fizer backup de `/dev/sda`, seu arquivo de imagem poderá não ser armazenado em `/dev/sda`.
4. Execute os comandos para criar um arquivo de imagem compactado:

```
dd if=/dev/SOURCE | gzip > /BACKUP_PATH/image.gz
```

5. Recupere o disco rígido usando os seguintes comandos:

```
gzip -dc /BACKUP_PATH/image.gz | dd of=/dev/SOURCE
```

Se você precisar de apenas uma partição para o backup, substitua o marcador *SOURCE* pela sua respectiva partição. Nesse caso, o seu arquivo de imagem pode usar o mesmo disco rígido, só que em outra partição.

30.6.2 Usando o sistema de recuperação

Há vários motivos pelos quais um sistema pode não ser inicializado ou executado adequadamente. Um sistema de arquivos corrompido após uma falha do sistema, arquivos de configuração corrompidos ou uma configuração de carregador de boot corrompida são os mais comuns.

Para ajudá-lo a resolver esse tipo de situação, o SUSE Linux Enterprise Desktop oferece um sistema de recuperação que você pode inicializar. que consiste em um pequeno sistema Linux que pode ser carregado em um disco de RAM e montado como um sistema de arquivos raiz, permitindo acesso externo às partições Linux. Com o sistema de recuperação, você pode recuperar ou modificar qualquer aspecto importante do sistema.

- Manipule qualquer tipo de arquivo de configuração.
- Verifique se há defeitos no sistema de arquivos e inicie processos de reparo automáticos.
- Acesse o sistema instalado em um ambiente de “mudança de raiz”.
- Verifique, modifique e reinstale a configuração do carregador de boot.
- Recuperar-se de um driver de dispositivo instalado incorretamente ou um kernel inutilizável.
- Redimensione as partições usando o comando parted. Encontre mais informações sobre esta ferramenta no site GNU Parted na Web http://www.gnu.org/software/parted/parted.html.

É possível carregar o sistema de recuperação a partir de várias origens e locais. A opção mais simples é inicializar o sistema de recuperação a partir do meio original de instalação.

1. Insira o meio de instalação na unidade de DVD.

2. Reinicialize o sistema.
3. Na tela de boot, pressione F4 e escolha *DVD-ROM*. Em seguida, escolha *Sistema de Recuperação* no menu principal.
4. Digite `root` no prompt `Rescue:`. Não é necessário inserir uma senha.

Se a sua configuração de hardware não inclui uma unidade de DVD, você poderá inicializar o sistema de recuperação a partir de uma fonte na rede. O seguinte exemplo aplica-se a um cenário de boot remoto. Se você estiver usando outro meio de boot, como um DVD, modifique o arquivo `info` adequadamente e inicialize como em uma instalação normal.

1. Digite a configuração do seu boot PXE e adicione as linhas `install=`*`protocolo`*`://`*`fonte_de_instalação`* e `rescue=1`. Se precisar iniciar o sistema de recuperação, prefira `repair=1`. Como em uma instalação normal, *`protocolo`* significa qualquer um dos protocolos de rede suportados (NFS, HTTP, FTP, etc.) e *`origem_inst`* é o caminho da origem de instalação da rede.
2. Inicialize o sistema usando "Wake on LAN", conforme descrito na *Book "Deployment Guide" 11 "Remote Installation" 11.3.7 "Wake on LAN"*.
3. Digite `root` no prompt `Rescue:`. Não é necessário inserir uma senha.

Depois de acessar o sistema de recuperação, você poderá utilizar os consoles virtuais por meio das teclas Alt–F1 a Alt–F6.

Um shell e muitos outros eficientes utilitários, como o programa de montagem, estão disponíveis no diretório `/bin`. O diretório `/sbin` contém utilitários de arquivo e rede importantes para análise e conserto do sistema de arquivos. Esse diretório também inclui os binários mais importantes para a manutenção do sistema, por exemplo, **`fdisk`**, **`mkfs`**, **`mkswap`**, **`mount`** e **`shutdown`**, além do **`ip`** e do **`ss`** para a manutenção da rede. O diretório `/usr/bin` contém o vi editor, find, less e SSH.

Para ver as mensagens do sistema, use o comando **`dmesg`** ou exiba o registro do sistema com **`journalctl`**.

30.6.2.1 Verificando e manipulando arquivos de configuração

Como exemplo de uma configuração que possa ser corrigida por meio do sistema de recuperação, suponha que você tenha um arquivo de configuração defeituoso que impeça a inicialização adequada do sistema. Você pode corrigir isso usando o sistema de recuperação.

Para manipular um arquivo de configuração, faça o seguinte:

1. Inicie o sistema de recuperação usando um dos métodos descritos acima.
2. Para montar uma sistema de arquivos raiz localizado em `/dev/sda6` para o sistema de recuperação, use o seguinte comando:

   ```
   mount /dev/sda6 /mnt
   ```

   Agora, todos os diretórios do sistema estão localizados em `/mnt`
3. Mude o diretório para o sistema de arquivos raiz montado:

   ```
   cd /mnt
   ```
4. Abra o arquivo de configuração problemático no editor vi. Ajuste e grave a configuração.
5. Desmonte o sistema de arquivos raiz no sistema de recuperação:

   ```
   umount /mnt
   ```
6. Reinicialize a máquina.

30.6.2.2 Reparando e verificando os sistemas de arquivos

Geralmente, não é possível reparar sistemas de arquivos em um sistema em execução. Se você tiver sérios problemas, talvez não consiga montar seu sistema de arquivos raiz e a inicialização do sistema poderá ser encerrada com "kernel panic". Nesse caso, a única maneira será reparar o sistema externamente. O sistema inclui os utilitários de verificação e conserto dos sistemas de arquivos `btrfs`, `ext2`, `ext3`, `ext4`, `reiserfs`, `xfs`, `dosfs` e `vfat`. Procure pelo comando **`fsck.`***`SISTEMADEARQUIVOS`*. Por exemplo, se você precisar verificar o sistema de arquivos `btrfs`, use **`fsck.btrfs`**.

30.6.2.3 Acessando o sistema instalado

Se você precisa acessar o sistema instalado do sistema de recuperação, faça isso em um ambiente *raiz de mudança*. Por exemplo, para modificar a configuração do carregador de boot ou executar um utilitário de configuração de hardware.

Para configurar um ambiente de mudança de raiz com base no sistema instalado, faça o seguinte:

1. Primeiro monte a partição raiz do sistema instalado e do sistema de arquivos do dispositivo (mude o nome do dispositivo de acordo com as suas configurações atuais):

```
mount /dev/sda6 /mnt
mount --bind /dev /mnt/dev
```

2. Agora, você pode "mudar a raiz" no novo ambiente:

```
chroot /mnt
```

3. Em seguida, monte `/proc` e `/sys`:

```
mount /proc
mount /sys
```

4. Por fim, monte as partições restantes no sistema instalado:

```
mount -a
```

5. Agora, você tem acesso ao sistema instalado. Antes de reinicializar o sistema, desmonte as partições com **`umount -a`** e saia do ambiente de "mudança de raiz" com **`exit`**.

Atenção: Limitações

Embora você tenha acesso total aos arquivos e aplicativos do sistema instalado, há algumas limitações. O kernel em execução é o que foi inicializado com o sistema de recuperação, e não com o ambiente de mudança de raiz. Ele suporta apenas o hardware essencial e não é possível adicionar módulos do kernel do sistema instalado, a menos que as versões do kernel sejam exatamente iguais. Verifique sempre a versão do kernel em execução (recuperação) com `uname -r` e, em seguida, descubra se existe um subdiretório correspondente no diretório `/lib/modules` no ambiente raiz de mudança. Em caso positivo, você poderá usar os módulos instalados, do contrário, precisará fornecer as versões corretas em outra mídia, como um disco flash. Na maioria das vezes, a versão do kernel de recuperação é diferente da que está instalada, portanto, não é possível simplesmente acessar a placa de som, por exemplo. Também não será possível iniciar uma interface gráfica de usuário.

Observe também que você sai do ambiente de "mudança de raiz" ao percorrer o console com as teclas Alt–F1 a Alt–F6.

30.6.2.4 Modificando e reinstalando o carregador de boot

Às vezes, não é possível reinicializar um sistema porque a configuração do carregador de boot está corrompida. As rotinas de inicialização não podem, por exemplo, converter unidades físicas em locais reais no sistema de arquivos Linux sem um carregador de boot ativo.

Para verificar a configuração do carregador de boot e reinstalá-lo, faça o seguinte:

1. Execute as etapas necessárias para acessar o sistema instalado como descrito em *Seção 30.6.2.3, "Acessando o sistema instalado"*.
2. Verifique se os arquivos a seguir estão configurados corretamente de acordo com os princípios de configuração do GRUB 2, descritos no *Capítulo 13, O carregador de boot GRUB 2*, e aplique as correções, se necessário.
   - `/etc/default/grub`
   - `/boot/grub2/device.map` (arquivo opcional, presente apenas se criado manualmente)

- `/boot/grub2/grub.cfg` (arquivo gerado, não o edite)
- `/etc/sysconfig/bootloader`

3. Reinstale o carregador de boot usando a seguinte sequência de comandos:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

4. Desmonte as partições, efetue logout do ambiente de "mudança de raiz" e reinicialize o sistema:

```
umount -a
exit
reboot
```

30.6.2.5 Corrigindo a instalação do Kernel

Uma atualização do kernel pode introduzir um novo bug capaz de afetar a operação do sistema. Por exemplo, um driver de parte do hardware no sistema pode estar com falha, o que o impede de acessá-lo e usá-lo. Nesse caso, reverta para o último kernel em funcionamento (se disponível no sistema) ou instale o kernel original pela mídia de instalação.

Dica: Como manter os últimos kernels após a atualização

Para evitar falhas na inicialização após uma atualização do kernel com defeito, use o recurso multiversão do kernel e indique ao `libzypp` quais kernels deseja manter após a atualização.

Por exemplo, para sempre manter os dois últimos kernels e o kernel atual em execução, adicione

```
multiversion.kernels = latest,latest-1,running
```

ao arquivo `/etc/zypp/zypp.conf`. Consulte o *Book "Deployment Guide" 8 "Installing Multiple Kernel Versions"* para obter mais informações.

Um caso semelhante é quando você precisa reinstalar ou atualizar um driver com defeito em um dispositivo não suportado pelo SUSE Linux Enterprise Desktop. Por exemplo, quando o fornecedor do hardware utiliza determinando dispositivo, como um controlador RAID de hardware, que precisa de um driver binário para ser reconhecido pelo sistema operacional. Normalmente, o fornecedor lança um DUD (Driver Update Disk — Disco de Atualização do Driver) com a versão corrigida ou atualizada do driver necessário.

Nos dois casos, você precisa acessar o sistema instalado no modo de recuperação e corrigir o problema relacionado ao kernel; do contrário, o sistema poderá não ser inicializado corretamente:

1. Inicialize da mídia de instalação do SUSE Linux Enterprise Desktop.
2. Se você estiver recuperando após uma atualização do kernel com defeito, ignore esta etapa. Se precisar usar um disco de atualização de driver (DUD), pressione F6 para carregar a atualização de driver depois que o menu de boot aparecer e, em seguida, escolha o caminho ou URL para a atualização de driver e confirme clicando em *Sim*.
3. Escolha *Sistema de Recuperação* no menu de boot e pressione Enter. Se você usar o DUD, será solicitado a especificar o local em que a atualização de driver está armazenada.
4. Digite `root` no prompt `Rescue:`. Não é necessário inserir uma senha.
5. Monte manualmente o sistema de destino e "mude a raiz" para o novo ambiente. Para obter mais informações, consulte a *Seção 30.6.2.3, "Acessando o sistema instalado"*.
6. Se você usar o DUD, instale/reinstale/atualize o pacote de driver do dispositivo com defeito. Sempre verifique se a versão do kernel instalada corresponde exatamente à versão do driver que está instalando.
   Se você estiver corrigindo uma instalação de atualização do kernel com defeito, poderá instalar o kernel original da mídia de instalação com o procedimento a seguir.
   a. Identifique o seu dispositivo de DVD com **`hwinfo --cdrom`** e monte-o com **`mount /dev/sr0 /mnt`**.
   b. Navegue até o diretório em que os arquivos do kernel estão armazenados no DVD, por exemplo, **`cd /mnt/suse/x86_64/`**.
   c. Instale os pacotes necessários `kernel-*`, `kernel-*-base` e `kernel-*-extra` de acordo com o seu tipo, usando o comando **`rpm -i`**.

7. Atualize os arquivos de configuração e reinicialize o carregador de boot, se necessário. Para obter mais informações, consulte a *Seção 30.6.2.4, "Modificando e reinstalando o carregador de boot"*.

8. Remova a mídia inicializável da unidade do sistema e reinicialize-o.

A Atualizações da Documentação

Este capítulo lista as mudanças no conteúdo deste documento desde a versão do SUSE® Linux Enterprise Desktop 11 SP3.

Este manual foi atualizado nas seguintes datas:

- *Seção A.1, "Outubro de 2014 (Versão Inicial do SUSE Linux Enterprise Desktop 12)"*

A.1 Outubro de 2014 (Versão Inicial do SUSE Linux Enterprise Desktop 12)

Geral

- Toda a documentação e as referências do KDE foram removidas porque ele não é mais fornecido.
- Foram removidas todas as referências ao SuSEconfig, que não é mais suportado (Fate#100011).
- Migrar do init do System V para o systemd (Fate#310421). A atualização afetou partes da documentação.
- O YaST Runlevel Editor mudou para Services Manager (Fate#312568). A atualização afetou partes da documentação.
- Foram removidas todas as referências ao suporte do ISDN, já que esse suporte foi removido (Fate#314594).
- Foram removidas todas as referências ao módulo DSL do YaST, pois ele não é mais fornecido (Fate#316264).
- Foram removidas todas as referências ao módulo Modem do YaST, pois ele não é mais fornecido (Fate#316264).
- Btrfs tornou-se o sistema de arquivos padrão para a partição raiz (Fate#315901). A atualização afetou partes da documentação.
- O **`dmesg`** agora inclui marcações de horário legíveis em formato igual a `ctime()` (Fate#316056). A atualização afetou partes da documentação.

- syslog e syslog-ng foram substituídos por rsyslog (Fate#316175). A atualização afetou partes da documentação.
- O MariaDB agora é fornecido como o banco de dados relacional, em vez do MySQL (Fate#313595). A atualização afetou partes da documentação.
- Os produtos relacionados ao SUSE não estão mais disponíveis em http://download.novell.com, mas em http://download.suse.com. Links corrigidos de acordo.
- O Novell Customer Center foi substituído pelo SUSE Customer Center. A atualização afetou partes da documentação.
- `/var/run` é montado como tmpfs (Fate#303793). A atualização afetou partes da documentação.
- As seguintes arquiteturas não são mais suportadas: Itanium e x86. A atualização afetou partes da documentação.
- O método tradicional de configuração de rede com `ifconfig` foi substituído pelo `wicked`. A atualização afetou partes da documentação.
- Vários comandos de rede foram descontinuados e substituídos por comandos mais atuais (**`ip`**, na maioria dos casos). A atualização afetou partes da documentação.

  `arp`: **`ip neighbor`**
  `ifconfig`: **`ip addr`**, **`ip link`**
  `iptunnel`: **`ip tunnel`**
  `iwconfig`: **`iw`**
  `nameif`: **`ip link`**, **`ifrename`**
  `netstat`: **`ss`**, **`ip route`**, **`ip -s link`**, **`ip maddr`**
  `route`: **`ip route`**

- Várias correções e adições pequenas feitas na documentação, com base em feedback técnico.

Capítulo 1, Atualização Online do YaST

- O YaST tem a opção de habilitar ou desabilitar o uso de RPMs delta (Fate#314867).
- Antes de instalar patches que exigem reinicialização, você é notificado pelo YaST e pode decidir como proceder.

Capítulo 3, YaST em modo de texto

- Informações adicionadas sobre como filtrar e selecionar pacotes no módulo de instalação de software.

Capítulo 4, Recuperação de sistema e gerenciamento de instantâneos com o Snapper

- Capítulo atualizado e novos recursos adicionados (Fate#312751, Fate#316238, Fate#316233, Fate#316232, Fate#316222, Fate#316203, Fate#316222).
- A *Seção 4.3, "Rollback do sistema por inicialização de instantâneos"* foi adicionada (Fate#316231, Fate#316221, Fate#316541, Fate#316522).

Capítulo 5, Acesso remoto com VNC

- O viewer do VNC padrão agora é `tigervnc`.
- Correções adicionadas sobre a inicialização do gerenciador de janelas nas sessões VNC persistentes.

Capítulo 7, Gerenciando software com ferramentas de linha de comando

- Documentação removida sobre o modo de compatibilidade com o rug do Zypper (Fate#317708)
- *Seção 7.1.5, "Consultando repositórios e pacotes com o zypper"* reescrita.

Capítulo 10, Inicializando um sistema Linux

- Capítulo reduzido substancialmente, pois o init do System V foi substituído pelo systemd. O systemd agora está descrito em um capítulo separado: *Capítulo 11, O daemon* `systemd`.

Capítulo 11, O daemon `systemd`

- Novo capítulo adicionado sobre o systemd e o Gerenciador de Serviços do YaST (Fate#316631, Fate#312568).
- Nova seção sobre carregamento de módulos do kernel (http://bugzilla.novell.com/show_bug.cgi?id=892349).

Capítulo 12, **`journalctl`***: consultar o diário do* `systemd`

Novo capítulo adicionado (http://bugzilla.novell.com/show_bug.cgi?id=878352).

Capítulo 13, O carregador de boot GRUB 2

- A documentação do GRUB Legacy foi substituída por um novo capítulo sobre o GRUB 2.
- O suporte ao LILO foi descartado.
- Nova seção adicionada *Seção 13.4, "Diferenças no uso de terminais no System z"*.

Capítulo 14, UEFI (Unified Extensible Firmware Interface)

- Capítulo atualizado e novos recursos adicionados (Fate#314510, Fate#316365).
- Função http://doccomments.provo.novell.com/comments/25080 .

Capítulo 16, Operação da impressora

Capítulo e seção atualizados de acordo com a nova versão do CUPS e com o PDF como formato de dados de impressão comum (Fate#314630).

Capítulo 18, O sistema X Window

- Capítulo atualizado para refletir a configuração dinâmica durante cada inicialização.
- *Seção 18.1, "Instalando e configurando fontes"* foi atualizada.

Capítulo 20, Rede básica

- O NetworkManager agora faz parte da Extensão de Estação de Trabalho: *Seção 20.4.1.1, "Configurando opções globais de rede"* (Fate#316888).
- Seção adicionada sobre a nova estrutura de **`wicked`** para configuração de rede: *Seção 20.6, "Configurando uma conexão de rede manualmente"* (Fate#316649).
- Outras opções mencionadas que podem ser adicionadas a `/etc/resolv.conf`: *Seção 20.6.2, "Arquivos de configuração"* (Fate#316048).

Capítulo 23, Samba

- Seção *Seção 23.6, "Tópicos avançados"* adicionada.
- Seção *Seção 23.6.1, "Compactação de arquivos transparente no Btrfs"* adicionada.
- Seção *Seção 23.6.2, "Instantâneos"* adicionada.

Capítulo 24, Compartilhando sistemas de arquivos com o NFS

- A configuração de compartilhamentos NFSv4 agora é muito parecida com o NFSv3, principalmente a configuração de montagem de vinculação que antes era necessária, mas agora foi descontinuada (Fate#315589).
- Seção removida sobre a configuração do servidor NFS.

Capítulo 25, Montagem sob demanda com o Autofs

- Capítulo adicionado sobre o `autofs` (Fate#316185).

Capítulo 28, Gerenciamento de energia

- Remova as referências obsoletas ao pacote `pm-utils`.

Capítulo 30, Problemas comuns e suas soluções

- Nova *Seção 30.3.4, "Não é possível montar a partição Btrfs raiz"* adicionada (Fate#308679, Fate#315126).
- Seção removida sobre o módulo de Conserto do YaST descontinuado (Fate#308679).

Configuração de Wi-Fi

- Capítulo removido sobre a configuração de Wi-Fi com o YaST, já que ela pode ser feita com o NetworkManager: *Capítulo 22, Usando o NetworkManager*.

Tablet PCs

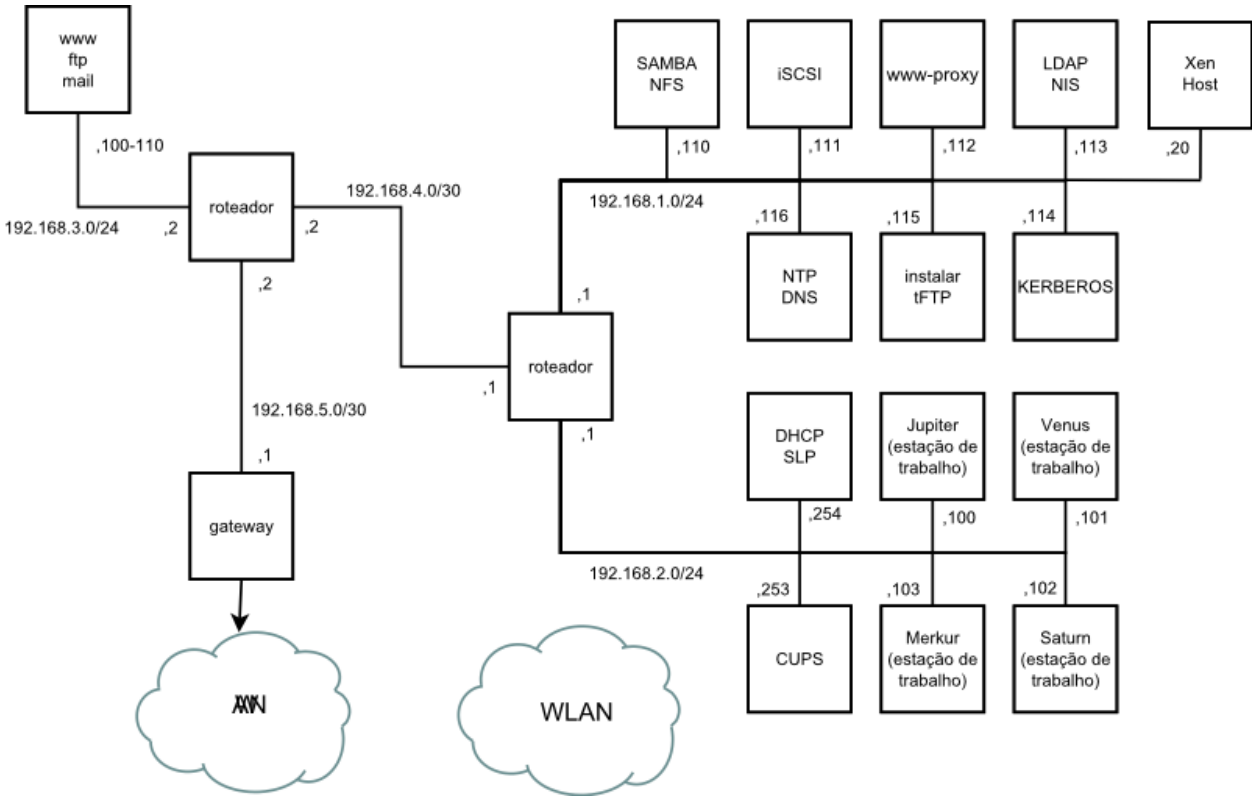
- Capítulo descontinuado removido sobre PCs tablet.

Correções de bug

- A seção foi adicionada *Seção 2.5, "Suporte aos módulos do Kernel"* (http://bugzilla.novell.com/show_bug.cgi?id=869159).
- Novo *Capítulo 12, **`journalctl`**: consultar o diário do `systemd`* adicionado (http://bugzilla.novell.com/show_bug.cgi?id=878352)

B Rede de exemplo

Este exemplo de rede é usado em todos os capítulos relacionados à rede na documentação do SUSE® Linux Enterprise Desktop.



C GNU Licenses

This appendix contains the GNU Free Documentation License version 1.2.

GNU Free Documentation License

Copyright (C) 2000, 2001, 2002 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from

which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

```
  Copyright (c) YEAR YOUR NAME.
  Permission is granted to copy, distribute and/or modify this document
  under the terms of the GNU Free Documentation License, Version 1.2
  or any later version published by the Free Software Foundation;
  with no Invariant Sections, no Front-Cover Texts, and no Back-Cover
Texts.
  A copy of the license is included in the section entitled “GNU
  Free Documentation License”.
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the “with...Texts.” line with this:

```
  with the Invariant Sections being LIST THEIR TITLES, with the
  Front-Cover Texts being LIST, and with the Back-Cover Texts being
LIST.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.